Strategies and Resilience Against Disinformation Influences

How Germany and Sweden respond to Russian disinformation

Conrad Timm

Abstract

In recent years the EU and its member states have seen increased activities of Russian disinformation influences impacting the national information environment. Germany and Sweden are interesting cases in relation to this issue as such hybrid threats target them both. This study aims to describe the national responses of the two countries in relation to Russian disinformation. A document analysis of government policies was conducted and combined with the theoretical framework of democratic deterrence and strategic narratives, which resulted in themes as a foundation for the analyses and discussion. As the countries are similar in nature and presented as such in the study, it is expected that they apply predominantly similar countermeasures. The results partly confirm this, however, they also show significant differences. The countries' approaches differ primarily in regulations aiming at controlling the dissemination of disinformation in the online environment. Additional differences make clear that Swedish policy documents better clarify the countermeasures of Sweden and thus are more informative about how to respond to Russian disinformation and hybrid interference in general. In contrast, the German policy documents are more discreet in terms of describing countermeasures, which makes it challenging to fully interpret and characterize Germany's countermeasures. In conclusion, the policy documents of Germany and Sweden differ in their description of countermeasures towards Russia and hybrid interference in general, which in a greater context impacts the informative quality and possible educational purpose of such policies. The results suggest that policy documents could be more explanatory and comprehensive for informative and educational purposes for relevant stakeholders and the public in general.

Key words: Disinformation, hybrid warfare, psychological defence, Russia, Germany, Sweden.

Words: 17.848

Acknowledgements

I would like to thank my supervisor Ketevan Bolkvadze for guiding me through the research-process and giving me inspiring and valuable feedback.
A special thanks goes to my family for the compassionate support, especially my sister for the important comments and helpful feedback at the end of the writing procedure.

Table of Contents

Abbreviations

EU	European Union
NATO	North Atlantic Treaty Organization
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
EEAS	European External Action Service
MSB	Swedish Civil Contingencies Agency
NetzDG	Netzwerkdurchsetzungsgesetz (Network Enforcement Act)
NGO	Non- governmental organization

1. Introduction

"Not long ago, the rise of social media-inspired great optimism about its potential for flattening access to economic and political opportunity, enabling collective action, and facilitating new forms of expression" (Guess & Lyons 2020, p.10). However, technological innovations and the upsurge and access to social media have not only given people in society a tool to organise and express themselves. Recent years have shown the harmful side of social media and the global information environment. Today, social media platforms are considered tools for spreading fake news and disinformation rather than being the medium for empowerment and social change (Ibid. p.10). The dissemination of disinformation online has strongly influenced the debate on democracy, elections, and public opinion in recent years. Disinformation is today a serious threat to our democracy, especially the spread of fake news online, which" [..] exploit social media to distribute disinformation, influence opinion and interfere in elections, posing a threat to democracy" (Saurwein & Spencer-Smith 2020, p. 820).

Nowadays, it is widely recognised among scholars and experts that digital technologies and the social media environment contribute to the polarisation in society. A straightforward example is that the social media environment can be an ideal environment to meet like-minded extremists. These digital technologies are used as tools and serve as echo chambers where the idea of a few individuals are amplified, reaching bigger susceptible audiences. The social media environment with its algorithms adapted to users' preferences generates filter bubbles and reinforces the political views and, at the same time, isolate users from consuming information that has an opposite character (Barberá 2019. p.34).

Hybrid warfare as a broad concept describes military and non-military tactics in war. Such tactics take advantage of applying many different modes of warfare within a given context, with the goal" to achieve synergistic effects in the physical and psychological dimensions of conflict' within the main battlespace (Hoffman, 2007, p. 8). Disinformation influences as a part of hybrid warfare is described as "..verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm" ((b) EU Commission, 2018). Further, Pascu & Vintila (2020) describe the issue adequately: "The main goal of the disinformation campaigns is to create an emotional decision-making environment to replace reason and factual-based judgment as a working method" (Pascu & Vintila 2020. p.61).

Recent years have clearly shown the increased activity of Russian disinformation influences targeting EU countries. Major recent events of Russia's hybrid warfare tactics include the annexation of Crimea, the interference and formation of opinions in the U.S. presidential election 2016 and elections in EU states such as the UK, Germany, and Sweden. In addition, Russia's links to the Facebook-Cambridge Analytica scandal in 2015 show how Russia uses its "hybrid toolkit", especially the dissemination of disinformation in its security strategies towards the EU and other western countries (EU Parliament 2019). These events defined a critical moment, as hybrid threats and disinformation influences made clear the vulnerabilities and unpreparedness of Europe and its Western allies (Jankowicz 2019, p.3; Colliver et al. 2018, p.2; Innes et al. 2021; EU Parliament 2019; Kalniete & Pildegovičs 2021, p.23).

These events make an interesting point of departure for studying disinformation influences targeting EU states. Furthermore, according to government policies and previous research, 2014 is mentioned as the year where disinformation activities increased (Bundesministerium des Innern 2016; Kragh & Åsberg 2017). Hence, 2014 serves as the point of departure for the analyses of the empirical material.

1.1 Purpose and research question

Considering the above mentioned, this paper aims to describe how two strong EU states, Germany and Sweden, respond to disinformation and hybrid influences emanating from Russia. Furthermore, what particular strategic countermeasures, that have not yet been studied in depth, the two countries apply. The ambition is to describe how countermeasures are reflected in policy documents and how the nexus of governments, state actors and other societal stake holders contribute to strengthen the resilience against disinformation.

The identified gap that drives this research is versatile. The research about disinformation and hybrid threats is relatively new. However, recent years have been decisive for the EU and its member states when it comes to being exposed to, identifying and counteracting disinformation and hybrid threats, which is reflected in news media, government policies and previous research. A majority of previous studies cover the topic of hybrid warfare and disinformation in relation to Russia, the development of hybrid warfare in the EU and the complexity of digitalisation and social media in relation to fake news and disinformation. However, the analyses of previous research clarify that qualitative case studies with a comparative purpose related to national countermeasures seem to be under-researched. Based on the identified issue, the question that guides the research is as follows:

- What is the nature of Germany's and Sweden's responses to disinformation influences emanating from Russia?

As the two countries are established as similar cases (as developed in the research design chapter), the expectations are that the national countermeasures against Russian disinformation are predominantly similar, concretely, that the stimuli (Russian disinformation)- response (countermeasures) should be similar in the two countries. However, it must also be assumed that differences in countermeasures exist, which the analysis of the empirical information also intends to discover. Germany is seen as the most affected country by Russian disinformation in the EU. In addition, previous research suggests that as a non-NATO member, Sweden stands out and is a more important target for disinformation influences than its Nordic countries, Norway and Denmark, as NATO members. This makes an interesting point of departure to research and describe the nature of both countries' responses to Russian disinformation (Deutsche Welle 2021; Deverell 2019).

In order to achieve the objectives of this paper, qualitative methods are used to identify and analyse the responses of government policies and societal resilience in each country in

combination with the theoretical framework comprising democratic deterrence and strategic narratives. The insights of this comparative research shed light on how far and in what way respective country has developed and applied strategies on an institutional and societal level, thus elucidating each countries strategic direction. On a broader scale, this research intends to contribute to more profound knowledge about how Western democracies communicate about and strategically respond to disinformation influences. This could benefit future research by adding to the bigger picture of hybrid activities directed towards Western democracies and affirm that democratic responses towards disinformation influences are the most important tools to counterbalance those threats, both from a governmental and societal level.

1.1 Definition of concepts

Below is an explanation of the different concepts used in this study which are extensively used in previous literature and policy documents. The EU Commission defines the concept of disinformation well for the context of this study:

> "Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary."

> (European Commission, 2018a).

'Hybrid warfare', sometimes also 'hybrid interference ,'hybrid tactics' or 'active measures' are more general terms. Hybrid warfare is defined as "an operational approach to warfighting that uses an explicit mix of military and non-military tactics" (Renz 2016. p. 283). Specifically, this can entail information warfare and psychological operations (Ibid. p.284). The chapters of the background and previous literature adhere to the terms as reflected in previous literature. Thus, 'misinformation' is defined as "constituting a claim that contradicts or distorts common understandings of verifiable facts" and thus "may be […] unintentional" (Guess, A.M. & Lyons, B.A., 2020. p.10,11). 'Disinformation' can be defined as a "subset of misinformation that is deliberately propagated " and is, therefore "meant to deceive" (Guess, A.M. & Lyons, B.A., 2020 p.11). As stated by the authors, these terms often overlap in definitions and are used interchangeably (p.10). Additionally, 'fake news' can be defined as false content and "deliberately misleading articles designed to mimic the look of actual articles from established news organisations" (Guess, A.M. & Lyons, B.A., 2020 p.11). 'Pro-Kremlin' and 'pro-Russian' are often used interchangeably and describe actors who act in line and support the politics of the Russian government and further the countries interests abroad. Lastly, 'resilience' in the context of this study describes how states and societies cope with external interference by working with strategies to counter them.

Throughout this paper, the term 'Russian disinformation' is used as the central concept and refers to the Russian information influences recognised in the online environment and news media targeting a country.

1.2 Thesis structure

Following the introduction part, chapter 2 describes the background and previous research. Chapter 3 introduces the theoretical framework. Chapter 4 explains the research design and clarifies the operationalisation of the findings. Chapter 5 categorically analyses the findings, which leads to the discussion and conclusion in chapter 6.

2. Background and previous research

In order to be able to carry out comprehensive research, it is essential to briefly analyse how each country is exposed to hybrid interference. This chapter briefly describes the nature of disinformation influence and countermeasures in relation to the EU and additionally continues with characterising the influence of Russian disinformation in the German and Swedish context. The EU strategy against disinformation is comprehensive and below text focuses on describing the essential strategies.

2.1 Social media and disinformation

The strategic manipulation that takes place on social media platforms is a serious threat to democracy, with a significant impact on trust in politics and institutions. Vaccari (2017) suggests that online mobilisation, which reaches a broader audience compared to offline mobilisation for the reason of low costs, increases political engagement among less attentive and relatively marginal citizens (p.85). With the help of conspiracy theories, fake news and hate speech, actors can mobilise electorates (p.2). A crucial role in this is the role of the major social media platforms, which, with their profit-driven algorithms, control the flow of information online. The so-called computational propaganda describes how actors use "…algorithms and automation whose task is to manipulate public opinion online" (Woolley and Howard 2018. p.2). Tools used in this propaganda to manipulate individuals and public discourse include coordinated disinformation campaigns, tactical leaks, automated political bots, and algorithmic micro-targeting (p.2). The ever-evolving technical developments and the ad-driven business models of social media platforms have a significant impact on public discourses and contribute to individuals' exposure to fake news and disinformation. The recent revelations of former Facebook employee Francis Haugen emphasise the current state of the biggest social media platform today. Haugen told a Senate subcommittee that "…I believe Facebook's products harm children, stoke division and weaken our democracy," and that Facebook and Instagram

algorithms, which tailor content that the users see, are causing harm and that the company chooses growth and profit over the safety of its users (The Guardian, 2021).

Durach et al. (2020) give a good overview on responses to fake news and digital transformation in and outside the EU. An exploratory qualitative study is used to analyse current countermeasures against information influences. The study analyses policy documents, reports and statements from Google, Facebook and Twitter from the EU Commission and EU Parliament. Further, laws implemented on a national level to counter disinformation. Finally, policies and programs connected to media education and fact-checking projects. The authors suggest four approaches to solutions for counteracting fake news and the dissemination of disinformation, further providing a picture of the pros and cons associated with these four solutions. The four areas constitute:" (1) self-regulation (i.e. actions undertaken on a voluntary basis by the digital platforms); (2) co-regulation (i.e. cooperation framework between EU-level and national-level authorities, the internet platform companies, media organisations, researchers, and other stakeholders); (3) direct regulation (i.e. legal measures & sanctions); and (4) audience-centred solutions (i.e. fact-checking and media literacy)" (Durach et al., 2020 p.5). In conclusion, the authors suggest that more co-regulation and improvement is needed in the context of digital platforms and their ad-based business models. With this, the power imbalance between the public authorities, the social platforms and policy-driven researchers can be improved while adapting regulations to each social platform model in the context of disinformation (Ibid. p.16). Their study contributes to a deeper understanding of different levels of possible solutions that are used to counteract disinformation in society. It also adds to the recognition that these solutions can be controversial, for example that measures taken by the state, when directly imposed can threaten press freedom and impose a form of censorship (Durach et al., 2020. pp.8, 15).

2.2 The nature of Russian hybrid tactics

The Russian hybrid tactics and information influences are widely recognized as a complex threat towards the EU and its member states. Information security is a crucial part of the Russian security doctrine. The development of the sector is a crucial objective for the Russian government that seeks to centralize information security forces at federal and regional levels and improve methods for cooperation among those forces. The Russian leadership can thus be described as supporting the strategic narratives towards Europe by using hybrid tactics by supporting political parties that oppose the idea of the EU and by supporting political movements that share common interests or have extreme agendas. As such, by using disinformation, the aim is to confuse and mislead, which weakens the public debate about specific issues, predominantly by controlling pro-Russian media which actively takes part in the Swedish and German news environment (Russian Government Doctrine of Information Security of the Russian Federation 2016; Hellman and Wagnsson 2017. p.156). As an example, Galoetti (2019) describes Russia's tactics as "aggressive geo-political campaign to assert its claims to great-power and also undermine western capacities to constrain it" (Galeotti 2019. pp 1-2).

2.3 Disinformation in the European Union

"The exposure of citizens to large scale Disinformation, including misleading or outright false information, is a major challenge for Europe. Our open democratic societies depend on public debates that allow well informed citizens to express their will through free and fair political processes"

(EU Commission 2018a. p.1)

Russia's annexation of the Crimean Peninsula in 2014 and the U.S. presidential election in 2016 are depicted as the main events where the problem of disinformation got increased political attention in Europe at the national and EU level (e.g., Saurwein & Spencer-Smith, 2020; Humprecht et al. 2020; Kalniete & Pildegovičs 2021). Most official EU documents describe hybrid threats and disinformation around the years 2018. For example, the EU Commission (2018) recognises hybrid threats and disinformation campaigns by foreign actors and, in relation to that, mentions Russia and its military doctrine in the document *Tackling online disinformation: a European Approach* (EU Commission 2018a). The mentioned problems and impacts described by the Commission are the spread of disinformation that affects policy development and public opinion and manipulates "societal debates and behaviour in areas such as climate change, migration policy, security, health, and finance" (EU Commission 2018a. p.2). Disinformation influences can significantly impact national elections, and safeguarding these is a task of the member states. However, a high-level expert group was tasked in 2017 to advise on the problem of disinformation in Europe as a common European approach is needed to tackle the cross-border threat of disinformation from foreign actors (Ibid. p.3).

The Commission outlines four general principles guiding the countermeasures against disinformation:

- First, to improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated and targeted in order to enable citizens to assess the content they access online and to reveal possible attempts to manipulate opinion.

- Second, to promote diversity of information to enable citizens to make informed decisions based on critical thinking through support to high-quality journalism, media literacy, and the rebalancing of the relation between information creators and distributors.

- Third, to foster credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers.

- Fourth, to fashion inclusive solutions. Effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement, and public authorities' cooperation, online platforms, advertisers, trusted flaggers, journalists, and media groups.

(Commission 2018a).

Furthermore, the following part gives a good idea of the complexity of disinformation and gives suggestions to be able to manage it in the online environment:

> "The mechanisms that enable the creation, amplification and dissemination of disinformation rely upon a lack of transparency and traceability in the existing platform ecosystem and on the impact of algorithms and online advertising models. Therefore, it is necessary to promote adequate changes in platforms' conduct, a more accountable information ecosystem, enhanced fact-checking capabilities and collective knowledge on disinformation, and the use of new technologies to improve the way information is produced and disseminated online."

(EU Commission 2018a. p.7).

Another area of focus concerning the countermeasures against disinformation is that of secure and resilient election processes, which can be manipulated by disinformation influences by way of hacking websites or disclosing personal information about politicians by getting access to personal accounts. Disinformation campaigns targeting elections can be used to endanger the integrity of publicly available information (EU Commission 2018a, Ibid. p.11). Another strategy is to foster education and media literacy, especially for young people, as a central tool to build a resilient society. Part of this is digital competencies and skills among various groups in society, for example, within the educational sector (Ibid. p.12). At last, strategic communication is essential to counter disinformation threats. It requires authorities to raise awareness and communicate about the issue and complexity of disinformation. It likewise includes countering disinformation and false narratives produced by the opposing actor, for instance, communicating about the EU and its policies. Active measures taken by the EU are among other the creation of EU Hybrid Fusion Cell 2016, which is part of the EU Intelligence and Situation Centre. Another is the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Since 2016, the EU and NATO have cooperated against hybrid threats, focusing on achieving a shared understanding and policy guidance, and the Hybrid CoE has a critical role in this partnership (Wijnja 2021; Hagelstam 2018). These reasonably new institutions monitor and deal with external hybrid threats and disinformation, which can negatively impact political decisions. The Hybrid Fusion Cell analyses and shares public and classified information within the European External Action Service (EEAS). The Hybrid CoE works with the capabilities of participating states to prevent and counter hybrid threats by cooperating with best practices, training and courses. This institution also provides a forum for NATO and EU collaboration. The financing of the different institutions and Directorate

Generals to tackle disinformation have varied much but increased significantly from 2015-2020 (EU Commission 2018a. p.15-16; EU Commission 2016; Hybrid CoE 2021(no date).

2.4 Russian disinformation in Germany and Sweden

Both Germany and Sweden have been exposed to disinformation campaigns emanating from Russia and are targeted similarly (Internetkunskap 2021; DW.com 2021). Below is an account of how Russian disinformation affects Germany and Sweden on a national level. This part considers what has been described as most influential in the previous literature and national policies on the subject.

Germany

A report by the EUvsDisinfo, a flagship project by the East StratCom Task Force, belonging to the EEAS, shows that Germany seems to be the main target of Russian disinformation in the EU. The report shows that 700 fake or misleading news cases have targeted Germany since 2015. France, in comparison, has been targeted 300 times, Italy 170 times and Spain 40 times (Deutsche Welle 2021; EU Observer (n.d.)). For example, a medium for this is the Russian sponsored state media RT (Russia Today), which reaches many Russian-Germans in the country (Applebaum et al. p.6).

Germany has seen increased Russian activity, such as state-sponsored media, in its elections in 2017. When it comes to Russian information influences and activities in Germany, many activities occur in the political discourse, especially around national elections. In particular, these Russian influences have a strong bond with the German party Alternative für Deutschland (AfD), and also, to some extent, left-wing politics and Russian-Germans (Applebaum et al. 2017. p.10). The AfD is the only party with a Russian campaign strategy and published Russian campaign material for the 2017 election (Ibid.p.16). This strategy serves as a gateway for Russian disinformation influence in the German social and political discourse. The tools used by Russia are Kremlin-sponsored media such as broadcasting media, social media networks and international far-right sources (Ibid.p.12). Well-known broadcasting media such as Russia Today (RT) and Sputnik play a significant role in spreading disinformation from Russia in Germany. During campaign periods before the 2017 election, the news reporting of German officials and institutions was consistently negative, while the AfD was not reported on in the same way. The most negative news was directed at Merkel, the German government and the police. In contrast, the Russian media channels choose to actively characterize the AfD as a mainstream party favoured by positive Russian news reporting. For instance, the Russian media channels use statements linked to the AfD party on their platforms, such as "rape is increasing due to Merkel's policy" (Applebaum et al. 2017. p.12). The Russian narratives are mainly based on stories about electoral fraud and immigration. This became visible when the AfD commented on social media that the party had been the victim of electoral fraud after an election in one of Germany's states. This was quickly reported by RT and Sputnik (Ibid. p.12). A further example was when various right-wing media pursued and distorted a narrative about news from Sweden where the Swedish police argued for better cooperation in problematic

areas. RT Deutsch reported on this, adding a twisted narrative that pointed to immigrants and Muslims as the problem of crime in these areas (Ibid. p.13).

The German left-wing party, Die Linke, also has a complex relationship with the Kremlin. The party has similar opinions of, for example, NATO and the United States as the Kremlin. Left-wing politicians also keep up good relations with Kremlin officials during trips to Moscow, and some politicians support Russian media in the form of appearances (Ibid. p.14).

The 2.5–3 million Russian speaking Germans are a vital audience and community for the Kremlin-affiliated media channels, especially prior to elections. The news broadcasted to this community distorts news and adds its narratives where Europe in relation to Russia is portrayed as weak. News can be classified as, for example, "Crisis of the European Union" or also "Western Plot Against Russia" (Applebaum et al. 2017. p.17). Furthermore, Sputnik DE and RT report on international and local political events in a partial way, which results in subjective news consumption by readers (Ibid. p.17). Another part of the distorted information flow takes place in Russian-German groups in social media, where a rich content of articles concentrates on immigration in Germany and attacks on Merkel (Ibid. p.18).

A further, more concrete example is the 'Lisa case', which exemplifies well how Russia uses propaganda and disinformation to influence public opinion. The story about a young Russian-German girl that went missing was picked up by Russian media, which reported an own version of the story, namely that the girl had been raped by immigrants. This went viral on social media and fuelled anti-migrant protests in the German-Russian community. In addition, Russian TV fuelled the tense situation more by reporting that the girl's claims were not being investigated. Thus, many protesters accused the German police of covering up the story. As the Russian foreign minister, Lavrov, got involved and strongly criticised the German authorities, the case became an international political issue. The girl later admitted that she had made up the claim of being raped. The refugee crisis was thus used by Russian propaganda to divide German society, emphasising that western society is not able to guarantee a safe environment for its citizens. Russia's involvement was seen as "Kremlin's attempt to manipulate public opinion in the West, stir up conflict and destabilise Western societies" (Spiegel, 2016; Knight 2016).

Sweden
In 2016, the then Swedish foreign minister, Wallström, mentions Russia's illegal annexation of Crimea and military presence in Ukraine as the biggest challenge against Europe's security order since the Cold War (Author's translation, Regeringskansliet 2016). Looking to Sweden, in their study about Russia's strategic influence, Kragh and Åsberg (2017) provide empirical evidence on Russians influences on Swedish policies in terms of public diplomacy and active measures since 2014, such as fake news and forged telegrams. The Swedish-NATO cooperation and Swedish support for Ukraine are two main areas affected by Russian strategic influences. A content analysis of the Swedish Sputnik news site outlines the main metanarratives of Russia's public diplomacy against Sweden (p.781). These metanarratives signify some consistent messages"…framing NATO as an aggressor and military threat, the EU as in terminal decline, and Russia as under siege from hostile Western governments" (Kragh & Åsberg, 2017. p. 806). The impact of Russian metanarratives can be seen in the Swedish media,

where Russian media use false news media published in Sweden to disturb the public's image of Sweden's political system. One of the most prominent narratives on Russia's part is the influence directed at Sweden concerning NATO. Russian officials have been openly critical to an increased Swedish NATO cooperation. Sweden's and NATO's special relationship has been reported frequently about in the Swedish Sputnik media considering the Swedish-NATO host agreement, which authorizes NATO to more efficiently operate in Sweden during training and conflict. In the Swedish case, Russia's most significant active measure and public diplomacy strategy are to disturb the close cooperation and integration with NATO (Kragh & Åsberg 2017. pp.797, 782,798).

Further active measures taken by Russia, which can have an impact within Sweden, include military threats, forgeries and disinformation, which in the Swedish information climate tend to be very sophisticated, showing a level of deep knowledge about crucial targets like Swedish officials, people within the diplomatic field and decision-makers. The authors argue that the Russian strategy and information impact intend to maintain the geostrategic status quo in relation to Sweden and the Baltics. Using active measures such as military threats, disinformation and security strategies aims to prevent a situation where NATO is more present. The authors conclude that it is hard to determine if Russian influence has any political impact and would be difficult to measure within a short time frame. However, the strategic goals and dominant narratives clarify that the influences are a well-coordinated campaign between Russian public diplomacy and active measures (Kragh & Åsberg 2017 pp.806-808).

Russian media channels such as Sputnik and RT play a significant role in the Swedish political and social discourse around the 2017 election. Unlike the German election 2017, where bots were used on Twitter to spread Russian disinformation, nothing comparable happened in Sweden during the election. However, in 2015 and 2016, there was an apparent increase in information campaigns and active measures, which could be related to, among other things, the increased Swedish cooperation with NATO. A thorough investigation made before the 2018 election shows increased reporting of Sweden by Sputnik and RT. As an example, between 16 July and 8 September 2018, these channels produced 520 news stories, and its international channels reported unilaterally on only the Pirate Party, Sweden Democrats (SD) and Alternatives for Sweden (AfS) (ISD 2018. p.12). Similar to the situation in Germany, news about these parties was presented in either a neutral or positive way, while the Swedish police and the government were presented in a negative or neutral tone (Ibid.). The pro-Russian media had a strong focus on reporting on migrants and crime as well as headlines about "failed integration policy, ineffective deportation procedures, presentation of asylum seekers and the Swedish Muslim community as a potential threat to national and EU security" (Colliver et al. 2018. p.14). During 2015-2018, Sputnik portrayed Sweden as a country with "growing internal contradictions" (Author's translation Hellman 2021. p.454). Furthermore, Sweden was described as having gone from a liberal and secure country to a country in political and moral decline (Ibid.).

In similar fashion to Germany, Russian backed media RT and Sputnik have both readers and contributors from the far-right, far-left and populist movements in Sweden. In relation to social media, the Russian online platforms VKontakte and Odnoklassniki have an indirect impact, where many far-right groups gain support among like-minded people, where Swedish

elections and Sweden as a whole are discussed, and in particular content about anti-immigration and a clear connection to the Sweden Democrats (SD) (Colliver et al. 2018. p.14). Another concrete example of active measures is a Swedish-Russian friendship organisation, which was reinvigorated in 2016. Part of the organisation where the Russian Embassy and communities in favour of pro-Russian agendas. The same community has been active in social media, supporting pro-Russian narratives criticising academics and journalists that write about Russian foreign policy (Kragh & Åsberg 2017. p.805). Russian hybrid warfare has developed in recent years in terms of, for example, increasing the budget for media funding. For example, the biggest beneficiary is Russia Today (RT), which increased its budget in 2017 from 261 million Euros to 325 million euros in 2020 (EUvsDisinfo 2018; 2019).

Deverell (2019) contributes with his comparative case study to the research of disinformation measures among the Nordic countries of Norway, Sweden, Finland and Denmark. The study contributes to a solid understanding of how Swedish authorities identify and counter disinformation and how Sweden stands in a Nordic perspective. The comparative case study is a qualitative analysis of policy documents, literature, and interviews with experts to show how the different countries work to identify and counter disinformation threats. Deverell concludes that Sweden, together with Finland, have established, organized and tested networks and organizations around the issue of disinformation earlier than Norway and Denmark. The empirical material also suggests that Sweden and Finland have been more exposed to disinformation influences concluded by the measures taken against it compared to Denmark and Norway. Of all the Nordic neighbours, Sweden has the most developed strategies and organizational structure on a broad scale to handle disinformation influences. This may be a result of the fact that the country is more sensitive compared to the other Nordic countries. Sweden's vulnerable side to disinformation influences is composed of the polarized debate about refugees and integration. This gives an opportunity for external actors to interfere in the societal debate between differing ideological opinions and amplify favourable arguments in order to exacerbate division. The integration question is often linked to EU sceptical opinions and the debate about a failed refugee crisis. As a non-EU state, Norway is not exposed to the same amount of disinformation influences. To argue and influence against a Swedish NATO membership are a part of the pro-Kremlin strategic narrative. As a NATO member, Norway is not exposed to the same amount of manipulative narratives. Deverell indicates that more systematically produced knowledge about disinformation is needed when analysing policy documents and strategies, which consolidates what other research suggests and what this paper aims to explore (Deverell 2019, pp.31, 45-49).

Russia's information impact can be analysed through antagonistic strategies (Wagnsson & Barzanje 2019) to categorize the information impact from pro-Russian media. Information influence directed towards Sweden assumes a destructive and diminishing discourse. Sweden is thus portrayed as a society in confusion, uncertainty, weak leadership and reduced trust (Hellman 2021. p.466). The strategy intends to disrupt and distort national discourses. Key concepts from experts and spokespersons are taken from various contexts and being modified, giving them incoherent and fuzzy meanings, which are then put against each other in a contradictory way. A good example of this is the misleading information about the Covid-19

crisis, where Russian influence activities are apparent. The pandemic has shut down many parts of society worldwide and made countries more vulnerable to hybrid influencers in the form of distorted news reporting, information influence and conspiracy theories (Hellman, 2021. pp.451, 466). In connection with this, it is essential to mention that the pro-Russian media do not directly publish incorrect information but use a misleading tactic where correct news information is given a different narrative or put together into narrative structures that benefit the pro-Russian media's goal of creating news and reporting about Sweden (Ibid. p.467).

Thus, what is the goal of the tactics mentioned above used by pro-Russian media, targeting states like Germany and Sweden? Information influences can impact a state's political polarization and give incentives and support for marginal groups and extremist movements. This can result in national security issues of violence in relation to these extremist groups. In addition, the international reputation of a country can be negatively affected by such polarization as the country is seen as unable to deal with internal issues and thus undermine the trust of the international community. Other consequences of the antagonistic narratives and the spread of rumours against may result in the country's leadership being questioned due to reduced trust and may affect the willingness among citizens and international partners to cooperate against external threats. For example in case of Sweden, the pro-Russian media uses the international and internal criticism about the country in handling the crisis to build on its own narratives and uses issues that divide society or that cannot be resolved in the short term (Hellman 2021. p.468).

3. Theoretical framework

This chapter introduces and exemplifies the theoretical concepts for this paper: resilience, strategic narratives and democratic deterrence. These concepts are operationalised to categorically analyse the empirical material and draw conclusions about the countermeasures in the discussion.

3.1 Resilience

One of the main concepts in previous literature important to this research is resilience. The concept of resilience is contextual and can have many meanings. In broader terms, it is related to how resistant states and societies are against potential collapse from disasters. Within the realm of disinformation research, it reflects state capacity, governance, support, and cohesion from society to its institutions and leaders. In essence, it describes how states and societies cope with external interference by working with strategies to deter, resist and overcome them (Kalniete & Pildegovičs 2021. p.26; Dunay & Roloff 2017. p.2).

As resilience is such a broad researched and used concept, it needs to be further defined in the context and use of hybrid warfare and disinformation research (Rhinard 2017). Rhinard thoroughly discusses the concept of resilience as he explains and problematizes the use of resilience in research and future policymaking. The concept was used primarily in biology and ecology before it was applied in policy analysis. Rhinard presents five key themes to clarify what the term means contextually.

1. "What is resilience?" – "Definitions range from the broad and expansive (the ability of any system – individual, household, community, organisation, state – to withstand, to adapt, and to quickly recover from stresses and shocks) to the narrow and specific (a community's ability to cope with a major disaster)" (p. 25).

2. "Who (or what) should be resilient?" - The question of who or what is resilient is clarified in the context in which the concept is to operate. It is emphasized that the individual capacity to adapt also determines how society or a state is resilient on a more integrated level. This can be an interesting starting point in analysing how societies and governments work to strengthen society on disinformation influences. For example, media literacy and obtaining a critical attitude when navigating in the information space is crucial for whether an individual contributes to the spread of disinformation or not. Furthermore, culture and experience play a role in how resilient an individual can be (p. 25).

3. "When can we expect resilience to happen?" - this aspect accounts for two angles of approach. Resilience seen from the traditional approach explains how, for example, a society 'bounces back' after being exposed to an extreme event. The second approach is included in more current research, where it is applied as something that happens before a disaster or other negative event. This can be seen as a more preventive aspect where the emphasis is on recognizing and adapting to potential future disasters (p. 26).

4. "What kinds of events do we hope to be resilient against?" - The arguments are twofold, where some focus is on the so-called "black swans" (unpredictable extreme events) are relevant in discussions and preparations for resilience. In the context of this research, we relate to and focus on normal circumstances and events where resilient systems are there to adapt and absorb the consequences (p.26).

5. "Can resilience be engineered?" - Is it worth preparing policy documents to create resilience? On a sceptical level, it can be argued that resilience is built up over a long period and is ingrained into society and built on experiences through exposure to disasters and negative societal impact. However, from an optimistic point of view, such policies in combination with effective leadership can be of value in creating resilience. (p. 26).

3.2 Strategic narratives

A more recent study by Hellman (2021) shows how Russian information influences in Sweden during the pandemic can have a negative domestic impact and damage the international reputation of a country. A narrative analysis of Sputnik news reporting resulted in four themes, which show how Russia uses tactics of suppression and destruction by pointing exaggerated and misleading covid related news and information about Sweden in order to depict the country as "a society characterised by insecurity, confusion, declining trust and weak leadership" (Author's translation, Hellmann 2021. p.466). The antagonistic strategies used in the analyses are based on a study by Wagnsson and Barzanje 2019, which explores Russian strategic narratives by exposing these with three different strategies: *suppression, destruction* and *direction* (p.239). By using a *suppressive* narrative, a state alters its status by damaging that of the other state. This can be achieved by using a country's status against itself, for example, Sweden, as a liberal, open and moral state with generous immigration policies, which can be scorned by storytelling in news media (p.250). The second strategy of destruction "…may undermine capabilities, making the 'other' appear weak" (Wagnsson and Barzanje 2019. p.250). The narrator's power is maximised and diminishes that of the other state. This is considered the harmful effect on an actor's power, its capacity for deterrence, military reputation and partnerships in military cooperation (p.250). In light of this, the affected state may be seen as a "weak power, an unattractive partner, a power that does not fit into a security community, a power with scant chances of generating military strength" (Wagnsson and Barzanje 2019. p.250). The study shows that there are stories about Swedish authorities not being able to control migration and crime in the case of Sweden. Swedish economy, demographic and military vulnerability and lack of allies are also depicted (p.251). The third narrative is *direction*, which "…through (implicit) inducements is a strategy of guiding the other away from an undesired posture, policy or behaviour, towards a preferred one through 'carrots' rather than 'sticks' " (Wagnsson and Barzanje 2019. p.251). This explanation of antagonistic narratives serves as a more underlying comprehension here. The below study elaborates more concretely on strategic narratives against hybrid interferences and thus accounts for a more elaborative aspect to the theoretical approach in this paper.

Hellman and Wagnsson (2017) offer a theoretical framework for analysing strategic narratives that explore how to respond to Russian hybrid warfare in terms of disseminating information influences. Both Germany and Sweden are included as examples of countries related to the strategic narratives. Four models are proposed that democracies can utilise as countermeasures: *Confronting, Blocking, Naturalising* and *Ignoring*. Two dimensions help put these models into a scale of engagement – disengagement and inward-outward targeting. Engagement means directly confronting the threat or narrative by an opposing actor by disseminating an own produced narrative, whereas disengagement provides for a passive position and a no-response policy (p.157). Inward and outward targeting "divides policies into those that primarily aim to target a domestic audience and those that target a foreign audience" (Hellman and Wagnsson 2017. p.158). It entails promoting the state to an external actor or public by applying narratives that give a positive image and achievement in the international arena, for example, power, reputation and contributes to different policy outcomes like

partnerships or trade agreements. Concrete examples that these strategies are aimed at are regions, neighbouring states or an international community. The inward-looking strategy aims to keep the domestic society free from external actors' influences and protect the national strategic narrative. In detail, this means hindering certain groups or individuals from taking part in public debate, censoring text or TV. Outward-looking involves the creation of counter-narratives aimed at targeting the interfering narrative as a direct response where to aim is "to promote the state and its worldviews thus gaining something in an international context; for instance, power, reputation or more specific outcomes such as trade agreements or entrance into security organisations such as NATO" (Hellman & Wagnsson 2017. p.158).

The confronting approach concerns the projection of counter-narratives, which poses a direct response towards a specific narrative. For instance, responding to false claims and manipulated narratives with the help of empirical evidence and reliable sources. Examples of this are Russian narratives targeting "events, leaders, people or phenomenon in European states" (Hellman & Wagnsson 2017. pp. 158,159).

In terms of *blocking* narratives, they can be well compared with the confronting approach, where a threatening narrative is acknowledged. Instead of producing a counter-narrative as a direct response, this approach aims at blocking the threat from outside to protect the own narrative. Concretely, this entails blocking information from the opponent, which gives them control of what domestic audiences are exposed to (p.161).

The *naturalising* approach is less engaging than the counter approach. Here, it is more important to promote the self-image as a country, not focusing on the *other*. It is about spreading the societal values and leading by example and "show foreign audiences a positive and appealing image of the nation and thus boost the state and its worldview in the long term" (Hellman & Wagnsson 2017. p.160). The authors give a pertinent example of how Germany responds to Russian disinformation. Germany recognises Russia as the primary source of disinformation targeting the country but does not directly counter the Russian narrative. Instead, Germany focuses on projecting its own positive narrative without getting involved in a debate and thus making the country look good (pp.159-160).

The *ignoring* approach gives no attention to an outside influence, meaning no engagement with a threatening narrative and is therefore disengaging. Instead, the aim is "to protect the domestic sphere" (Hellman and Wagnsson 2017. p.162). The approach relies on the state and its democratic resources like institutions and government agencies and the ability to defend the open society against threatening narratives. This entails strengthening civil society and empowering citizens to be critical within the media environment and contribute to the societal debate (Ibid.). The authors suggest that Sweden adopts an ignoring strategy as a consequence of trust in the democratic institutions and their capability of managing the threat of information warfare that the society is exposed to (p. 162).

The authors also suggest that it is most likely the case that states use several of these strategies to counter foreign narratives. For instance, Germany assumes a more naturalising approach but gets involved in a more blocking narrative by supporting TV channels in the Baltic countries that confront Russian narratives (Sturm 2016, p.164). Similarly, Sweden mixes its strategic narratives by being more confrontative by working against Russian narratives in the East StratCom Task Force (Ibid. p.164).

The study provides an interesting insight into what strategies can be used to handle disinformation. A clear analytical framework is presented to clarify how countries can develop and improve their national strategies for dealing with internal and external disinformation influences. The strategic models and dimensions will be used as a theoretical framework in this paper to describe which strategies are used in Germany and Sweden.

Engagement **<** ————————————————————————**>** Disengagement

Confronting   Blocking   Naturalizing   Ignoring
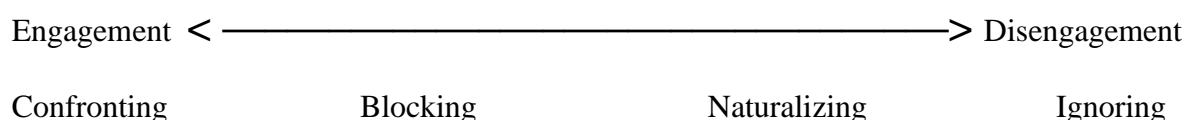
(Hellman & Wagnsson 2017**)**

3.3 Democratic deterrence

Another important theoretical contribution is presented by Wigell (2021) and specifies how Western democracies should counteract hybrid interference. The fundamental point of departure is that traditional military-based deterrence is more compatible with purely military threats than the hybrid threats to which many Western democracies are exposed. It is also a matter of responding to these threats in a way that is both in line with democratic values and also in a non-escalating way. Democratic deterrence is suitable for understanding what counter-strategies Germany and Sweden use as both countries rely on democratic solutions against disinformation activities. Democratic deterrence depends on a whole-of-society approach, implying that the state has a governing responsibility, but where public and private social actors cooperate in gathering all democratic resources to respond to hybrid threats, such as disinformation. Social actors are thus an essential part of the functioning of a society in crisis. Moreover, based on a soft-power approach, democratic norms and values become a strategic tool for dealing with actors who have an authoritarian character (Ibid. pp. 52-53).

Within the theoretical framework of deterrence, the concepts of *denial* and *punishment* have their roots in traditional military deterrence. Democratic deterrence instead adopts the expressions *resilience*, which is rooted in denial and *compellence*, rooted in punishment (Ibid. p.55). This new approach also means that the strategies used to strengthen society and meet antagonistic forces must not sacrifice the democratic openness of the Western world for the sake of security (Ibid.) The strategies *of expanding sanctions* (compellence) and *increasing transparency* (resilience) do not find any significant support in the empirical material and are thus only briefly mentioned here but are not considered as analytical tools in the analyses.

Deterrence by denial – improving democratic resilience

The concept of resilience has been defined in the literature review. The concept is reiterated as a part of democratic deterrence. To improve democratic resilience, Wigell emphasizes three different approaches; *activate civil society, increase transparency* and *broaden inclusion.*

Activate civil society is about how civil activism and market-based innovation can help identify and build social structures and thus contribute to strengthening resilience. This broadly inclusive approach involves working with everything from media literacy programs and training for civilians and journalists to developing rapid alert systems (p.56). Increasing access to open data also means that private and civilian actors who are not tied to the state can work with obtaining intelligence and revealing hybrid threats (p.57).

Broaden inclusion includes the entire population in building societal resilience by making everyone aware of hybrid threats. This is done by ensuring broad political participation and improving social welfare to reduce gaps and improve societal stability. This may be particularly directed at minorities and diasporas, which in some cases can be used as agents for foreign powers' hybrid activities (p.59).

Increasing transparency is about disrupting collaborations between foreign actors and domestic groups in their work to pursue common agendas. This also means that financial support and investments from foreign actors must be controlled more (p.58).

Deterrence by punishment - Discovering democratic compellence

The effectiveness of democratic deterrence is assured by democratic compellence. Wigell states: "At present, hybrid interference largely goes unpunished—and as long as this is the case, interference remains a highly tempting and potentially effective strategy" (Wigell 2021. p.60). Hence, democratic compellence functions not only via sanctions and diplomatic tools but also through democracy itself since authoritarian regimes have shown to be "terrified by democracy and the threat it poses to authoritarian control" (Wigell 2021. p.6). The approaches for this strategy as communicating response thresholds, expanding sanctions and promoting democracy.

Communicating response thresholds is about what counts as unacceptable behaviour with consequences towards actors of hybrid interference, which means that Western democracies must be able to identify and respond to hybrid threats, for example with sanctions or other measures. An essential part of this is discrediting existing actors and reminding such actors of the strength of independent media and civil society as a watchdog while naming and shaming is a common practice and puts pressure on governments to counteract (p.60).

Promoting democracy is another strategy of democratic compellence that uses the soft power of democracy as an advantage to respond with force to hybrid threats. This entails, for example, working with truth against the propaganda that comes from authoritarian regimes to respond to and challenge its narratives (p.62). In practical terms, this means, for example, working with revelations about corruption. This can be related to the Russian leadership's assets held in the West, which should not come under possible scrutiny at home, which can be used as a means of negotiation (Ibid.). A further approach is to strengthen the program that works with human rights and democracy to influence and support the network and society in other countries that are based on democratic values such as cultural institutions. Strengthening civil

society from a bottom-up approach is something that authoritarian regimes want to avoid, so it can be of great importance to building democracy with civil society groups in countries such as Russia (p.63).

Expanding sanctions concerns the possibility and strength Western democracies can display by using sanctions. All states are dependent on global trade, resources and information to protect their security and prosperity, which is to a majority controlled by Western democracies, which in turn can set up such sanctions and other countermeasures. Cooperation among Western democracies with sanctions as a tool is necessary to strengthen deterrence and, in extreme cases, to apply them against authoritarian foreign actors (p.61).

Wigell argues that both deterrence by denial (resilience) and deterrence by punishment (compellence) is necessary to stop hybrid interference (p.55). However, for the analytical part of this paper, democratic deterrence is in itself incomplete to stand alone as an analytical tool as the research of previous studies reveals that more categories are needed to analyse the countermeasures of both countries. Therefore, with democratic deterrence as the central theoretical part, *state resilience* and *regulation* were added as themes and are used to categorize and analyse each country's countermeasures and assess the national situation (see table under 5.5). In addition, the framework of strategic narratives presented by Hellman and Wagnsson (2017) adds another theoretical aspect to the beforementioned framework to clarify and position each country's strategic narratives.

The theoretical framework presented in this chapter serves as a tool for analysing the findings to understand and explain how the chosen cases, Germany and Sweden work with countermeasures. Democratic deterrence and strategic narratives thus serve as frameworks and build up the thematic categories in the analyses. The theoretical approaches combined give extra strength to the analyses and complement each other well as democratic deterrence serves as the basis in the analyses, and strategic narratives further elucidate and position the countries strategic narratives.

4. Research design

This chapter describes the choice of case studies in relation to the qualitative research, the collection of empirical material and the operationalisation of this paper, with a conclusion of the limitations of this approach. This paper is deductive and exploratory in nature as the focus is to use existing theoretical aspects to analyse the empirical information. In general, qualitative exploratory research is among other aspects conducted when the available theory is inaccurate or incorrect. This aspect is adopted for this research as two existing theoretical aspects are combined in order to explore and contribute to the research issue (Creswell & Creswell 2018. p.104; George, T. 2021).

4.1 Qualitative Comparative case study

Qualitative research aims to make sense of empirical data and identify patterns and themes to build up and depict a picture that helps answer the research aim. Qualitative research is a phenomenological interpretation where human senses and subjectivity inevitably plays into the research process (Leung 2015. p.324). This research aims to get a deeper understanding of how two strong EU countries counter Russian disinformation. A qualitative approach is best suited for this type of research and document analysis serves as the chosen strategy for gathering empirical data as it takes on an interpreting and descriptive character.

Germany and Sweden are in this paper presented as similar cases in the context of how they are expected to deal with and counter Russian disinformation. Thus, the expectations are that similarities in countermeasures are to be found at both the governmental and societal levels for both countries. The similarities considered here are that both countries are strong European democracies with sophisticated societies and with an open economy, which anticipates that they are exposed to the same kind of hybrid threats and show comparable vulnerabilities (Wijnja 2021. p.15). In addition, the countries also have a strong public broadcasting service and established media, which is a fundamental component in dealing with disinformation, suggesting a strong societal resilience. The trust in public broadcasting and established media is high among citizens and is similar in both countries.

The choice of Germany and Sweden adopts a most similar cases method, also known as the most similar system design (MSSD). In the most classic form of this method, all independent variables of both cases are similar except for the independent variable of interest, meaning that the cases of choice are as similar as possible except for the phenomenon that the research attempts to assess. The strict application of control variables to the cases is one way of implementing a MSSD. However, this paper adopts a looser application of the MSSD, meaning that this paper will not systematically match the cases on possible variables. Instead, the strategy is for the countries of choice to have as many similarities in their background characteristics as possible. The choice of applying a loose MSSD in this paper and not to include independent and dependent variables enables a broader and more unrestricted study of the research aim (Seawright & Gerring, 2008. p.304; Anckar 2006 p.389; Newman et al. 2021. pp.80,104; Speck 2020).

The method of interpreting the empirical data takes on a thematic analysis approach, which is used to analyse qualitative data and identify themes in the empirical material. By using this approach, the purpose is to "identify patterns of meaning across a dataset that provide an answer to the research question" (Braun & Clarke, 2019, para. 9). Hence, this is connected to a step-by-step process that guides the analyses, which do not pose as strict rules to follow but are rather seen as tools. These tools are familiarisation with the data, coding, generating initial themes, reviewing themes, defining and naming themes and writing up. Mentioning these tools is essential for the understanding of what thematic analysis is. However, this research will not follow every step explicitly as it is neither the aim nor is it feasible to code every sentence or paragraph in the chosen policy documents. However, this is not a disadvantage of the research process as it does not assume a semantic approach used to find out the exact content but rather a latent approach that should emphasise concepts and underlying assumptions. From the very

beginning, the research process is guided by themes (countermeasures, strategic narratives, resilience), making the process take on a deductive approach (Braun & Clarke, 2019).

4.2 Document analysis

Documents are analysed and interpreted to gain a deeper understanding and meaning and develop empirical knowledge (Bowen 2009. p.27). A wide variety of documents are considered for document analysis, in this case, reports, public documents, books, scientific journals. The systematic procedure of gathering relevant information entails finding, selecting, making sense and combining material to shape reliable data. Document analysis is considered an intense study of material that suits well for qualitative research, as it yields a deep understanding of a single phenomenon or event (Ibid. p.29). The content of documents is also relevant for the background information and historical understanding. One example in the context of this paper is scientific journals, as they often take into account historical events as background information. Another aspect is that the content of documents gives new insights, which leads to new observations and suggestions and forms the research. Since the documents are issued over time, for example, government reports, they provide valuable insights into temporal developments related to disinformation and hybrid interference in general (Ibid. p.30). The researcher is very well acquainted with the language and culture of both Germany and Sweden, which is advantageous for the research of national policy documents as some of them are written in either the German or the Swedish language.

4.2.1 Advantages and disadvantages of document analysis

Document analysis can be seen as beneficial as the gathering and analyses of the material is less time-consuming. It is seen as an efficient research method emphasising the selection rather than the collection of data. The public availability of the documents gives researchers the ability to choose carefully from a wide range of material spanning over time. In addition, documents are stable and unaffected by the research process in contrast to, for example, observations that can be impacted by the observer (Bowen 2009. p.31).

The drawbacks of document analysis can be that documents are not produced for research, resulting in that the material studied is not as detailed and satisfactory as the researcher needs it to be. Another aspect is an incomplete collection of material resulting in 'biased selectivity' (Yin 1994. p.80). However, Bowen (2009) clarifies that the benefits of document analysis exceed the drawback considering the efficiency and the low cost of such research (p.32).

The documents will be analysed and reviewed thoroughly to find the most relevant information. This leads to the categorisation and the selected data to form themes for the analyses. The process requires attention to detail of the various documents as it is crucial to keep an objective mindset, pursuing a balanced representation of the data (Ibid. p.32). When critically evaluating the documents, the research should look for meaning and how the data contributes to a further understanding of the context. Relevance, authenticity, accuracy and

representativeness must be assured. A relevant question is related to the number of documents considered for analysis. Bowen indicates that the quality rather than the quantity of documents should be considered, even though a multitude of documents can serve the purpose of bringing evidence to the research (Ibid. p.33). This paper first and foremost considers the most relevant documents to provide the research with substantial context and uses further documents, like previous research, to verify and solidify the findings. The analysis of documents should be used to evaluate and produce empirical knowledge and at the same time strive for objectivity and sensitivity (p.34). The risk of being too biased in data selection is mitigated by the limited amount of the official documents and reports available and relevant for this research (Yin, 1994).

4.3 Data selection

As described in the introduction, this paper is based predominantly on material depicting the period 2014-2020. Other sources have been chosen to add to the analyses because of the limited empirical material in the German policy documents (as interpreted in the discussion). The purpose is to find and emphasise main strategies in policy documents. The reports analysed for both countries are primary security documents and other relevant policies that reflect the national position on hybrid warfare, disinformation and information influences.

First, documents from government and state actors in each country have been chosen to provide substantial knowledge about the governmental action taken. Documents produced by governments and state actors are collected from web pages of, for example, the Swedish Government, Swedish Civil Contingencies Agency (MSB, Myndigheten för Samhällskydd och Beredskap,) or the German Governments webpages. The majority of documents are either in Swedish or German, except for documents that exist in an English version. The reliability of these sources is high and sets the scene for a further selection of documents and relevant information. Documents chosen for this criteria clearly outline national security strategies that bring up countermeasures in different varieties. In its nature, the work against disinformation is shaped by government policies, which means that working against disinformation adopts a top-down approach as it is a matter of national security to develop responses and inform the public. Other documents that serve to give a deeper understanding of disinformation and hybrid warfare are scientific articles derived from the Lund University database and Google Scholar. The analyses of both types of documents give a balanced, informative overview in the sense of specifying government strategies and, at the same time, outlining the scholarly work in the field.

Selection criteria are applied to provide a fair and balanced overview of selected empirical material. A majority of the documents usually cover a period of more than one year and are not always produced on an annual basis by, for example, a country's government or a national research institute. Arguably, this can be seen as a disadvantage in the selection of materials for the continued empirical research process. However, the intention is not to account for research-relevant material on an annual basis but to find the most relevant and essential empirical material. In relation to this, there may be a natural imbalance between the number of documents from each country. However, by systematically reviewing the selected documents, it is ensured

that each country is represented in a balanced way as far as it is possible. In addition, the variety and broad scope of the collected material makes the material sufficient for the interpretations of the research. Finally, the combinations of policies, academic journals and NGO reports assure the balanced assessment of the research problem.

Institutions and organizations whose main task it is to work against and inform about disinformation are the primary sources of information. The documents produced by these actors vary in terms of relevant content. The exploration of the empirical material has shown a substantial diversity of documents that depict the subject of countermeasures. Many do so on a more general level, and therefore the documents chosen for the analyses are the ones that are most relevant to the subject considering the aim of this research. The different amount of policy documents for each country reflects the purposeful balance intended to reflect each countries position as reliable as possible. The documents are used to various extents both in the background and previous literature as well as in the analysis. Complementary documents and information from web pages are added in the analyses to add more strength. This is especially related to the context of Germany, as the analyses clarified the limited empirical information about the countermeasures.

Below are the primary documents, which were extensively analysed for this research. However, only the most relevant documents of these are used in the analyses. The reason is that for both countries, a part of the documents, for example, the *Verfassungsschutzbericht* by the German Domestic Intelligence service or *Strategic Outlook* from the Swedish Defence Research Agency, are limited in useful content. This is especially the case for the German documents. This issue is further developed in the discussion.

Germany

- Verfassungsschutzbericht 2014, 2015, 2016, 2017, 2018, 2019, 2020 (Reports by the German domestic intelligence service).
- Weißbuch 2016 (White paper on German Security Policy and the Future of the Bundeswehr, German Government).
- Die Lage der IT -Sicherheit in Deutschland 2020 - Bundesamt für Sicherheit in der Informationstechnik (The IT security situation in Germany 2020 - The Federal Office for Information Security).
- Shaping Digitalization' 2021 presents the digitalization strategy of the German federal government (added complementary information).

Sweden

- Strategisk utblick- Totalförsvarets forskningsinstitut nr. 6 2015, nr. 7 2017, nr. 8 2019, nr. 9 2021 (Complementary information) (Strategic Outlook from the Swedish Defence Research Agency).
- Myndigheternas arbete med psykologiskt försvar 2017 (The authorities' work with psychological defence 2017).
- Statens Medieråd lägesrapport 2020 (The Swedish Media Council's status report 2020)

- Det demokratiska samtalet i en digital tid 2020- Statskontoret (The democratic conversation in a digital age' 2020 – Swedish Agency for public management).
- Sveriges nationella säkerhetsstrategi 2017 (Sweden's national security strategy 2017).
- Countering Information Influence Activities 2018 (MSB).

Key Word Analysis

In order to get a proper perception of the chosen documents, they were searched with the keywords depicted in the table on the next page. This resulted in an overview in order to point out to what extent the content in the documents contributes with insights into countermeasures relating to Russian disinformation. This processes also assures the relevance, authenticity, accuracy and representativeness of the documents (Bowen 2009. p.33). The selection criteria for official documents for the relevance of this research derives from the search with keywords such as 'disinformation', 'disinformation influence', 'disinformation campaigns', 'resilience', 'hybrid threats" hybrid warfare',' information activities',' Russia' and' Russian'. The search with the keywords has been carried out in such a way that the omission of important context has been avoided, for example, 'Russ' (Russia), 'counter' (counter influences, countermeasures- in Swedish' motstånds-xxx',' påverkans-xxx'). The corresponding keywords are introduced in the table below. After extensive reading and analyses of the empirical material, the keywords were chosen and are used as reliable and applicable analytical tools. The keywords are used in both the German and Swedish languages to find the most relevant documents, also for the search in databases. The measure of relevance of an official government document is decided by a clear intention of the document linked to the research purpose, such as a research report "Countering Information Influence Activities" from MSB, which contains valuable information. To further assure the applicability of the content, a search with the keywords in the document is performed, which results in a clear overview of the content. For example, a 60-page document that includes only four matches on the word 'disinformation' together with three matches on the word 'Russ*' (Russia) are not suited to be a leading source of empirical material. In contrast, documents containing, for example, 23 matches on 'disinformation' and 20 matches on the word' Russ*' are considered valuable.

The relevance of documents varies by nature. The selection of the most applicable information available relies upon using the selection criteria as a tool, thus ensuring how the data creates meaning for the research context considering the authenticity and representativeness of the issue discussed (Bowen, 2009). The words described below are not equally represented in each country's documents, and considering the different languages, some words are used to a greater extent than others. This is unproblematic as the process of reading and selecting documents has clarified that some words are used much more in certain documents than others and vice versa.

Table 1. Keywords used to determine relevance of content

English	Swedish	German
Disinformation	Desinformation	Disinformation
Disinformation influences	Desinformationspåverkan	-
Disinformation campaigns	Desinformationskampanjer	Desinformationskampagne
Resilience	Motståndskraft	Resilienz
Hybrid threats	Hybridhot	Hybride Bedrohungen
Hybrid warfare	Hybrid krigföring	Hybrider Kriegführung
Influence campaigns	Påverkanskampanjer	-
Information activities	Informationspåverkan	-
Russia /Russ*	Ryssland/Ryska/Ryss*	Russland/ Russ*
Counter* (measures)	Motstånds* (-kraft/anda)	Gegenmaßnahmen
Preventive	Preventiv	Prävent* (prävention/präventive)

4.4 Operationalisation

The interpretative part of the research process includes summarising, comparing, and discussing the findings from a personal view and giving suggestions for further research and limitations where the researcher should reflect on the lessons learned. Such lessons could be, for example, if the findings derive or confirm previous information? Or if new questions have arisen from the collected data that was unforeseen? (Creswell & Creswell 2018. pp.198-199). The comparison of Germany and Sweden in this case study may result in such lessons and will be discussed in the conclusion. Operationalisation makes sense of and links the concepts and themes with the empirical evidence gathered in the research process (Lowndes et al. 2018. p.227).

The theoretical framework, consisting of democratic deterrence, strategic narratives and resilience, serves as the foundation for the analytical part. The themes below will be interpreted through the lens of these theoretical concepts to describe each country's situation. The empirical data chosen (as described above in the part of data selection) is analysed systematically. Finally, the documents on which the empirical material is based will be analysed through the themes to get a categorical insight into how Sweden and Germany respond to Russian disinformation influences. The state level describes countermeasures taken by the government, including regulations aiming at tackling disinformation and also includes state resilience. The societal level describes societal resilience, which includes the aspects of education and media. Significant parts of these consist of awareness of disinformation in education and the role of public media and news. The table below gives an overview of the themes that are pre-determined for the analyses and derive from the theoretical framework.

Table 2. Theoretical framework

Theoretical lens Democratic Deterrence	Themes	Theoretical lens Strategic narratives
Democratic compellence- (deterrence by punishment)	-State resilience -Regulation -Communicating response thresholds -Promoting democracy	Ignoring and naturalising (covers the whole analytical chapter)
Democratic resilience (deterrence by denial)	-Activating Civil Society, Broaden Inclusion -Media and Education	

4.5 Reliability, Validity and Generalizability

Validity and reliability have a partly different meaning in qualitative research than that characterized by quantitative research. In qualitative research, validity means "appropriateness of the tools, processes, and data" (Leung 2015. p.325). This relates to if the research question is valid for the outcome, if the correct research design and methodology have been chosen and if the results are valid for the context (Ibid.). The research design and methodology for this research are deliberately chosen to answer the research question. The appropriateness of the strategies and processes used to find and assess the empirical material is carefully chosen to ensure high qualitative research.

In contrast to quantitative research, where reliability refers to the exact replicability, reliability in qualitative research relates to a consistency where a "margin of variability for results is tolerated" (Ibid. p.326). Hence, a researcher needs to ensure that consistent and stable approaches are used for the case study procedure (Creswell & Creswell 2018. p.201). The data selection procedure and document analyses have been carried out in a consistent and systematic form to ensure reliability. For instance, the search for relevant documents has assumed a top-down character where first government documents from most relevant actors have been taken into account. The findings illustrate the overall national strategy against information influences and relate to empirical material linked to other societal actors and their documents.

In terms of generalization, the primary intent of qualitative research is to focus on particularity rather than generalizability, thus focusing on a specific phenomenon in a particular context (Creswell & Creswell 2018. p.202; Leung 2015. p. 326). Although this research attempts to gain more profound knowledge of a specific context between two cases instead of providing generalizable results, there might be value in comparing the findings on a broader

level, thus contributing to a more comprehensive understanding of hybrid threats and disinformation influences impacting EU countries.

4.6 Limitations

Critically considered, qualitative studies are sometimes seen as too subjective and impressionistic, which means that qualitative results are often based on unsystematic perceptions of what is essential. In relation to quantitative research, where the problem formulation tends to be somewhat more precise, qualitative research in the starting phase can instead assume a more open character and thus rather specify the research puzzle and questions at a later stage (Author's translation, Bryman 2008. p.368). In qualitative research, the researcher (and his or her feelings, interests and perspectives) is central to how research is steered and how the empirical material is collected. In relation to quantitative research, where these factors are rather seen as undesirable, in qualitative research, these factors can be seen as an advantage by enriching and adding extra scope to the result (Leung 2015. p.324). Furthermore, a replication of qualitative studies is associated with difficulties as these usually assume an unstructured character and have influenced much of the researcher's approach, creativity and interests (Author's translation, Bryman 2008. p.368). The limitations in this research can be linked to the asymmetry of the representation of the documents that depict each country. As anticipated and described under the subsection 5.4, even if choosing the most relevant documents depicting each countries situation, there might be a marginal imbalance that naturally occurs as there are different documents about the issue in question. A systematic analysis counterbalances this to ensure a strong validity and reliability.

5. Analysis

This chapter intends to describe and compare the findings for each country with the theoretical framework of *democratic deterrence* combined with *strategic narratives*. As posed by Wigell, "Western democracies urgently need to find countermeasures against hybrid interference […] (Wigell 2021. p. 52). Democratic deterrence clarifies and describes different aspects of dealing with hybrid interference and "suggests a novel way of thinking about deterrence to dissuade these hybrid interference activities by authoritarian states" (Wigell 2021. pp.52-53). The findings are presented as different themes derived from Wigell's suggestions in combination with themes constructed for this paper- *state resilience* and *regulation*. A concise analyses of the findings in relation to strategic narratives aims at describing each countries' strategies against Russian disinformation and foreign interfering narratives in general.

5.1 Democratic Compellence

5.1.1 Germany

State resilience

Considering the above mentioned more limited findings for the German part, one of the primary informative policy documents is the White Paper 2016. The paper outlines the overall national security strategy. More specifically 'hybrid threats' and 'resilience' are mentioned a number of times in the document. However, they are not developed on a deeper level, whereas 'disinformation' is non-existent. Countermeasures and strengthening the resilience must have a whole-of-government approach to security. Along these lines, it is of great importance to increase "cooperation between government bodies, citizens and private operators of critical infrastructure, as well as the media and network operators" (White Paper 2016. p.48). Moreover, "the objective of resilience is to improve the ability of both state and society to withstand and adapt to disruptions, such as those caused by environmental disasters, severe system failures, and targeted attacks. The objective is to enable the state, the economy and society to absorb adverse events while continuing to function" (White Paper 2016 p.49). To successfully prevent hybrid threats, a state and whole-of-society approach is needed to strengthen resilience, which is achieved by connecting different policy areas, protecting critical infrastructure and having a common approach among politicians, media and society to expose propaganda with facts (Ibid. p.39). Germany also focuses on building long-term resilience together with allies and partners as "enhanced resilience at international level will also benefit security at the national level" (White Paper 2016. p.60). Concretely, The German strategy also relies very much on the cooperation and joint exercises with NATO in the realm of hybrid threats, strategic communication and cyber security (Ibid. p.75). In connection with the German approach, *Propaganda Awareness* is a project initiated in 2018 within the Bundeswehr and aims at countering propaganda and disinformation targeting the army with the help of research, analysis, defence and resilience (Bundesministerium der Verteidigung, 2020*).*

The White Paper 2016 outlines the German security policy comprehensively. However, Russia in connection with hybrid activities is only briefly mentioned in connection with an account of how the picture of Russia has changed after the crisis in Ukraine and Russia's role in the international arena, such as the UN. It is described that with the annexation of Crimea, Russia has shown readiness to go its own way and with the use of hybrid warfare and violence in eastern Ukraine, the country is intensely challenging the European peace order that has been built up over decades. The European Community, which rests on a strong vision of security in Europe, has been built up as a result of multilateral cooperation and a strong set of common values. The events in Ukraine show that Russia is turning against that security architecture in Europe and is becoming a strategic rival. Furthermore, the document acknowledges the increased Russian military activities on the borders with Europe and that Russia's use of hybrid methods is problematic for the peace order. The problem requires answers from NATO, the EU and the member states (White Paper 2016. p.32). Germany's relationship with Russia is briefly described in the context that Germany has worked for a strategically important and cooperative

relationship with the country. It is further emphasized that Germany has to find the correct balance between collective defence together with increased resilience and at the same time cooperative security and sectoral cooperation in the relations with Russia (Ibid. p.32). Germany is also working for a long-term relationship between NATO and Russia. Due to the Crisis in Ukraine, Russia shows sides both through deterrence and military capabilities but also the readiness to engage in dialogue (Ibid. p.66).

The German Ministry of Foreign Affairs also plays a vital role in working against disinformation influences. The Ministry for Foreign Affairs has presented new strategies for defending the common European narrative. This will be done through modernization and diversification of various communication tools simultaneously as experts will be hired to analyse Big Data and hire more employees for strategic communication (Digital-made-in.de 2021).

Regulation

In comparison to Sweden, Germany has gone a step further to control the social media environment and introduced stricter requirements on social media actors by introducing the Network Enforcement Act. The law was introduced in 2017 and is one of the strictest requirements on how large social media platforms must deal with harmful content. Thus, harmful content must be removed from the platforms within 24 hours after receiving a complaint. In June 2021, the NEA was amended to increase the user-friendliness of complaints about illegal content, introducing an appeal procedure to review flagged content decisions and requiring that the annual transparency reports must contain more information (Library of Congress, 2021; Gorwa, 2021). However, NetzDG is not a complete set of rules against disinformation and has also been criticised as being ineffective against harmful and illegal content, as "disinformation often operates in a legal borderline area, which makes it unclear exactly what is covered by freedom of expression, and what is in fact illegal." (Jaursch, 2019. p.2).

Communicating response threshold

The most compatible empirical findings within this approach, is the above mentioned NETZ DG, which can be seen as a threshold to disseminating disinformation as a part of hybrid interference. Although it does not necessarily match the approach suggested by Wigell entirely, it can be categorized as an indirect response of thresholds. Further, other most compatible findings can be derived from how the German government reacts to disinformation influences which entail the work of public relations departments to monitor fact and social media, hence adopting a preventive and reactive approach. However, in relation to this, "setting thresholds is a difficult matter since there is a risk to lose credibility if a government does not stick to earlier announcements" (Wijnja 2021. pp. 12-13).

Promoting democracy

By nature, this approach adopts a vast category of democratic tools. One important aspect is that of fact-checking organisations where the German government has increased cooperation with social media platforms and organisations that work with fact-checking (Wijnja 2021, p.11). In Germany, both public service and private media companies use fact-checking to handle fake news and disinformation. Nonetheless, it has been shown that fact-checking as a tool against misinformation is not as effective as anticipated. With fact-checking, only the symptoms of disinformation are treated, but not the root causes, the reason being that disinformation and fake news reach a much larger number of people than fact-checking itself does (Sängerlaub 2018. p.1). The strategy of using fact-checking counters foreign false narratives and thus works with the truth against disinformation intended to distort public opinion. This contributes to upholding democratic debate in society and further the promotion of democracy.

5.1.2 Sweden

State resilience

Sweden's countermeasures against disinformation influences are tackled at a broad societal level. It consists of three steps: *Becoming aware of information influence, identifying information influence* and *countering information influence* (MSB 2018). Sweden's strategy adopts a cross-sectoral approach, which includes many societal actors. Many political areas and authorities are included in this, such as culture, digitalisation, and media policy. Politics and authorities thus contribute to jointly strengthening resilience. The overall concept of Sweden's work against disinformation influence is reflected in the total defence (totalförsvaret). According to law, the total defence is the military and civilian operations needed to, in the worst-case, prepare the country for war (Regeringen, 2015a). Due to the deteriorating external environment, the Swedish Government commissioned in December 2015 the Armed Forces, MSB and other civilian actors to "resume coherent planning for the total defence (Author's translation, Regeringen 2015b). The Government decision also emphasises Russia's actions to contribute to a deteriorating security policy situation in Europe, especially considering the events in Ukraine. The risk of military threats has thus increased in Sweden's immediate area, which means that a new focus on defence and Sweden's international security policy cooperation is enhanced (Regeringen 2015a; SOU 2020:56).

The organisation in Sweden with the major responsibility of organising and working against disinformation is the Swedish Civil Contingencies Agency (MSB), which has the overall task of identifying and countering the impact of disinformation. This is done through external monitoring and analyses of how disinformation affects Sweden. Since 2009, MSB has been tasked with creating coherent information on the total defence and security policy. On a concrete level, businesses and societal actors are given information to work proactively to identify and manage possible security threats and information impact. In order to be able to

identify threats and impacts and work with security measures, a developed collaboration between authorities and other societal actors is required. In connection to this, it is also emphasised that the national security strategy will partly be based on the NIS Directive. The directive is the EU's common legislation that ensures strategic cooperation between member countries, the countries preparedness to face challenges by, for example, a Computer Security Incident Response Team (CSIRT) and a security culture that extends to all sectors of society such as healthcare, infrastructure and energy. Concretely, MSB has published "Countering Information Influence Activities- a Handbook for Communicators" (2018), which is aimed at informing people who work in public administration and relevant organisations (MSB 2018; Commission 2021;Statskontoret 2017:5, p.24).

One of the most significant measures is the government decision (early 2021) to create an Agency for Psychological Defence (Myndigheten för psykologiskt försvar), which began with the Government appointing an investigation in 2018 for a new agency that is going to work with "strengthen the overall ability to identify and meet improper information influence and other dissemination of misleading information directed at Sweden" (Author's translation, MSB 2021). The agency's main task is to coordinate, develop and support societal actors and authorities in the work with psychological defence since a modern psychological defence spans several sectors of society and that cooperation is required between many different public and private actors (MSB 2021; SOU 2020:56. p.131). The authority also has the task of "strengthening the population's ability to detect and resist influence campaigns and disinformation" (Author's translation, SOU 2020. p.131), which also means to "ensure the population's will of defence in peace and will of resistance in war" and to "ensure that objective public information can be conveyed quickly and efficiently even under disturbed conditions and to identify, analyse and counter campaigns of influence. The psychological defence must also, as far as possible under disturbed conditions, ensure an open and democratic society with freedom of opinion and free media" (Author's translation, Justitiedepartementet 2018:80. p.*7)*. The Agency for Psychological Defence shall cooperate with the Armed Forces, the security police, the police authority and authorities within the judiciary as part of the total defence (totalförsvaret) (Ibid. p.9).

In 2016, the Government commissioned the 'Swedish Agency for Public Management' (Statskontoret) to "report on the activities conducted by Swedish state authorities that are relevant to a psychological defence adapted to the current situation" (Author's translation, Justitiedepartmementet 2016 (11:8). p.1). The research would contribute to the Government's work to develop government activities regarding psychological defence. Therefore, it was essential to identify the crucial authorities contributing to a psychological defence. The reason for this decision was the deteriorating external situation and the opportunity for foreign actors to influence Sweden negatively by spreading "disinformation and rumours to influence attitudes and actions among individual centrally located decision-makers or among the population" (author's translation Justitiedepartmementet 2016 (11:8). pp.1-2). In this decision, the Government also clarifies by a *principle of responsibility* (ansvarsprincip) that it is the responsibility of each actor "to identify and meet the information influences within their respective areas of responsibility" (Author's translation, Justitiedepartmementet 2016 (11:8). p.2).

Communicating response threshold

At the beginning of 2018, the Swedish government presented further measures to strengthen society against disinformation influences, especially threats emanating from Russia. This was done at a broad societal level and included many actors who could strengthen the resilience. The government communicated that it continues to build up a modern total defence (*totalförsvar*) and part of it, a psychological defence adapted to the current threats directed at Sweden. Particular focus was placed on the election, which was to take place in September of the same year. MSB, the Security Police and the Police Department carried out vulnerability analyses. Furthermore, the various political parties received information and participated in a meeting on the risks of information influence and how to increase protection against such threats. Media actors were also invited to discuss and collaborate on possible influences before the election. Sweden also contributed with staff for EEAS and NATO StratCom COE to help manage Russia's information impact (Statsrådsberedningen 2018).

Promoting democracy

A concrete example for this approach is that the Swedish government spends SEK 10 million annually for increased freedom of expression and the work against disinformation in the Baltic Sea area. As proposed in the Budget Bill 2022, the financing of 10 million annually will continue as it has done since 2017. The initiative contributes to strengthening actors who work for freedom of expression and counteracts disinformation (Regeringskansliet 2021). Additionally, the various initiatives of educating the public on disinformation and how to navigate in the online environment is a significant contribution to the promotion of democracy as elaborated on in the next chapter.

Regulation

As already established, Sweden has no regulations in place contrary to the German Netz DG. This is also confirmed by the comprehensive report *The democratic conversation in a digital age 2020,* where it is stated that "However, the various democratic challenges that the social platforms have given rise to are pervasive and different models of self-regulation cannot obviously be considered sufficient. Against this background, the Committee believes that an inquiry should be set up to analyse how democracy is affected by global platform companies, as well as whether legislation may need to be developed to safeguard democracy in the long run" (SOU: 2020:56 p. 20).

5.2 Democratic Resilience

In the following part, the approaches of *activating civil society, broadening inclusion* and *media and education* are analysed together as media and education is a powerful tool to build societal resilience (activate civil society) and societal awareness (broaden inclusion). It makes sense to combine them as they are closely associated with each other and therefore give a more solid analysis.

5.2.1 Activating Civil Society, Broaden Inclusion - Media and education

Germany

The analysis shows that the German documents do not elaborate satisfactorily on the part covered under the societal aspect. Therefore, complementary documents and web pages have been used that describe the civil society approach in the best possible way.

In Germany, The Federal Agency for Civic Education is one of the central agencies to inform about disinformation. As in Sweden, Germany aims for a society with increased resistance to disinformation (BPB 2021. p.174). This is achieved with the help of *trust, awareness, reflection* and *empowerment*, which build a foundation for increased resilience (Ibid. p.175). The document from The Federal Agency for Civic Education covers the topic of disinformation comprehensively. However, it focuses mainly on the individual responsibility of citizens to navigate critically in the online environment and does not elaborate on concrete counter strategies on a societal level.

The most concrete proposals for increased resilience and media literacy can be found in the document 'Shaping Digitalisation' from 2021. Education in compulsory school, further education at other levels and the creation of a competent society are the main points. The various ministries, such as the Federal Health Ministry (BMG) or the Federal Ministry of Education and Research (BMBF), are responsible for carrying out the objectives. The projects are dedicated to strengthening digital competence in healthcare professions, to strengthening media competence in children, young people and adults in order to ensure a secure upbringing with digital media. Many projects are also aimed at girls and women to increase security in the online environment (Die Bundesregierung 2021. pp.13-18). For example, The Federal Ministry of Family Affairs, Senior Citizens, Women and Youth (BMFSFJ) is monitoring digital competence in society in order to contribute with insight for the scientific, educational and workers community in order to develop more targeted educational tools for strengthening digital competence (Ibid. p.17).

Sweden

Within the realm of digitalisation politics, several efforts are being made to strengthen media and information literacy. The Ministry of Infrastructure bears the responsibility at the state level. More robust countermeasures are about using new technology and ensuring good conditions for the digital infrastructure (SOU 2020: 56. p.115). One of the five sub-goals in the digitalisation strategy is digital competence, which is a prerequisite for digital participation in society. Digital security is also an important aspect that must provide the precondition for everyone in society to be able to participate in the digital society in a safe way (Ibid. p. 115). Within the education sector, the work towards increased resilience is about conducting more fundamental work, such as emphasising issues within democracy and human rights. Sweden's municipalities and regions (Sveriges kommuner och Regioner, SKR) have developed an action

plan based on the digitalisation strategy for the school system, which means that students must develop their skills in media and information literacy. The aim is for the Swedish school to be a leader in digitalisation in order to contribute to a high level of digital competence among students (SOU 2020:56 p.119).

A significant part of the psychological defence is described with the concepts a *spirit of resistance (motståndsanda)* and a *willingness to defend (försvarsvilja)*. Strengthening the spirit of resistance is about the population's attitude and the individual's willingness to resist in times of peace and war. This is based and depends on trust in the state and the armed forces and solidarity in society. Building trust in peacetime is seen as a fundamental prerequisite for identifying and countering disinformation (SOU 2020:56 p. 23). Authorities and other societal institutions must work to build trust in society as a high level of institutional trust among citizens contribute to a stronger spirit of resistance and a willingness to defend values and society itself. A high level of trust from the population improves the conditions for authorities to counter disinformation (Ibid p.23). Furthermore, it is described that the will to defend, which means how Sweden should use its military resources in the event of threats or attacks, can be strengthened within the framework of psychological defence through increased knowledge of security policy and total defence in society (Ibid. p.25).

Furthermore, in psychological defence, the media play a crucial role by mediating news and being part of society's information system. The Media Contingency Council (Mediernas Beredskapsråd), as part of MSB's work, is an important link in this context. It brings together various media actors to be able to act quickly in the event of a crisis. Furthermore, it brings together knowledge of threats, risks, vulnerabilities, strengths, and available resources discussed among the council members (MSB 2020; Statskontoret 2017: 5 p.25).

A survey from 2017 clarified that about 80 per cent of the authorities conduct activities that can be linked to some part of the psychological defence, while only a third of these believe that they play a role in relation to this (shown by interviews). This points to a lack of knowledge regarding the psychological defence among authorities and demonstrates that the government must clarify its expectations of the authorities' work (SOU 2020:56 p. 41). Regarding resisting and countering disinformation, many actors contribute to identifying these threats, such as the armed forces, intelligence services and the police authority. Their work is to conduct systematic environmental monitoring and increase knowledge about disinformation and its dissemination in society (Ibid. p.54).

Media and digital competence are described in several government documents. They reflect the goals required to strengthen the media competence in Swedish society. This is done through a digitalisation strategy that increases the digital competence and security of the population, a digitalisation strategy for the educational system where children and students must develop their digital skills. Libraries also play an important role in awareness about the need to increase digital competence. A strategy for a strong democracy is critical for increasing digital competence for the democratic participation of the population (Carlsson 2018. p.109). Target groups for strengthening the digital and participation are often elderly and newly arrived people. However, given the broad impact that disinformation influences have, digital competence needs to be strengthened towards a much broader target group (Ibid. p.110).

A status report by the State Media Council emphasizes the work for increased digital competence by the individual's responsibility to navigate safely in the online environment. Concretely, the individual should be vigilant in the consumption of online information. Furthermore, it appears that the State Media Council, based on the two government assignments, has established a structure in society that provides an opportunity to develop skills further and strengthen knowledge "that is necessary for people's autonomy and democratic participation in a digital present and future" (Author's translation, Statens Medieråd, 2020. p.29). However, establishing a social structure for media and information literacy must be a long-term work where many actors will contribute and collaborate to raise the quality of work for increased digital competence (Ibid.).

5.3 Strategic Narratives

Below is an analyses of Germany's and Sweden's strategic narratives as reflected in the primary policy documents.

Germany

German strategic narratives adopt a mixing strategy with both *naturalising* and *ignoring* characteristics. Naturalising, because Germany is focusing more on the self-image instead of building up strategies in order to confront Russian disinformation. For example, a strong focus is on educating citizens in media competence and raising awareness about increasing security when navigating in the online environment. In both the White Paper 2016 and other policy documents, Russia is not directly confronted and denounced as a problematic foreign actor. Instead, with strategies of regulation (Netz DG) and fact-checking, societal values are upheld and strengthened in order to increase resilience against actors such as Russia. This confirms Helmann and Wagnssons (2017) example of Germany's response to Russia. Likewise, the ignoring approach is reflected in the little amount of attention directed at the foreign narrative of Russia. Instead, it emphasises how Germany works with institutional capabilities to defend and strengthen the society against Russian narratives.

Sweden

Sweden adopts a mixing strategy with both an *ignoring* and *naturalising* approach. In terms of ignoring, Sweden's strategy is disengaging, and much focus is on protecting the domestic sphere. The newly established Agency for Psychological Defence with the task of coordinating and managing the threat of disinformation shows Sweden's strong institutional approach to countering disinformation. Sweden focuses on strengthening civil society and raising awareness which includes many societal actors like businesses and organisations. Information is communicated to these actors to raise awareness of how disinformation is spread and strategies to identify and handle such threats. A concrete example is MSB's Handbook for Communicators (MSB, 2018). *The naturalising* approach can be recognised in Sweden's *total defence,* which as a comprehensive and long-term method against hybrid interference implies

the priority on spreading the societal values and focus on promoting the national self-image. The findings also confirm what Hellman and Wagnsson (2017) described that Sweden cooperates against the Russian hybrid within the EEAS and NATO StratCom COE, making the country adopt a more confronting approach (p.164).

This concludes that both the German and the Swedish approach is disengaging in nature, focusing on more inward-looking measures by protecting the national strategic narrative, spreading and consolidating societal values and increasing resilience by educating and empowering citizens. Furthermore, the primary strength of both countries is the societal trust and reliability in institutions, the government and national media, which together build a strong unity of countermeasures.

6. Discussion and conclusion

The purpose of this paper was to analyse the nature of Germany's and Sweden's countermeasures against Russian disinformation as described in policy documents. As the countries are presented as similar cases, the initial expectation was that they would apply predominantly similar responses. However, the research has brought several interesting findings, which partly confirm the expectations and also point out differences.

Considering the similarities, the policy documents for both countries affirm that the majority of disinformation influences emanate from Russia as the primary source of foreign interference within the international and national information environment. However, the countermeasures described in the policies do not reflect back precisely to Russia as a foreign actor of hybrid interference. The policy documents for both countries show a weak link between Russian disinformation and countermeasures aimed explicitly at Russia. Rather, they show a strategy against disinformation and hybrid interference in general, which consequently targets Russia as well. The countermeasures are neutral and describe how each country is prepared and works against any hybrid interference, regardless of the interfering actor. Thus, it can be concluded, that in accordance with policy documents, the link between the 'stimuli' (Russian disinformation) and the 'response', (countermeasures) are insignificant.

Furthermore, the findings confirm what Hellman and Wagnsson (2017) described in relation to the countries' strategic narratives. Namely, that they adopt mixing strategies of *naturalising* and *ignoring* national responses. Instead of countering specific hostile narratives, they are aimed at strengthening and protecting the domestic narrative and build societal resilience. In terms of resilience-related to both the state and societal part, the expectations were thus partly confirmed. The countries show a very similar approach when it comes to adopting a whole-of-government and a whole-of-society approach to build a stronger resilience.

Considering the abovementioned, the remaining part of the discussion is focusing on the differences between the countries and how countermeasures are emphasized in policy documents.

The Swedish policy documents show more transparency and are more concrete about which societal actors and agencies are working with strategies against disinformation and hybrid threats. For example, it is well reflected in the policy documents that the Agency for Psychological Defence and MSB are the leading agencies in Sweden responsible for societal cooperation and countermeasures against disinformation influences. Furthermore, the Swedish policies emphasize and communicate the national strategies in a more apparent way by reason of Sweden's approach of defending transparency and free flow of information (Hellman & Wagnsson, 2017 p.166). Consequently, it clarifies much more the Swedish governmental position and national counterstrategies against disinformation and hybrid interference in general.

For Germany, the information about countermeasures is much more discreet and unspecific, and the policies reveal a much vaguer description of countermeasures. This makes it more demanding to draw conclusions about Germany's specific strategies and countermeasures compared to Sweden. This has been improved by including additional information. Wijnja (2021) confirms what the analysis of German documents has revealed during the research process. Namely, that there is not much information about countermeasures against hybrid threats reflected in official policy documents (pp.12-13). A concrete example is the yearly reports from the German domestic intelligence service (Verfassungsschutz). These documents could be expected to have high relevance to the issue of disinformation, especially in relation to Russian foreign politics. The reports from 2014-2020 show that hybrid warfare in relation to Russia is described only in general terms. Russia is acknowledged as a foreign actor using hybrid methods like disinformation campaigns, economic influence and influencing Russian diasporas in Germany (Verfassungsschutzbericht 2019 p. 317). Considering that concrete countermeasures against disinformation and hybrid interference are vaguely described, it can be concluded that the documents are unspecific in nature, especially in comparison to the Swedish equivalent.

What is significant for Germany, are the regulations implemented in the social media environment where Germany has adopted a stringent law and Sweden still seems to maintain an ambivalent position. The German regulatory initiatives control and potentially reduce the spread of harmful content like disinformation and fake news. It also puts the Swedish strategy in strong contrast where such regulations are non-existent at the moment. The Netz DG regulation serves as a pertinent example of how a national legislative initiative contributes to controlling and minimising exposure to fake news, hate speech and disinformation on social media. Considering that the Netz DG was established in 2017, it seems that Sweden has a different approach to something that has been an essential tool in Germany for a couple of years.

The findings demonstrate that the approaches that Wigell suggests are not fully reflected in the policy documents. This is more obvious for the German part in the analyses where it was challenging to match national countermeasures in relation to Wigell's suggestions. Consequently, this further confirms that the German policy documents are vaguer and contain informative content only on a general level. In addition, the parts of *expanding*

sanctions and *increasing transparency,* did not find any support in the empirical material for both countries.

Furthermore, the themes *communicating response thresholds/ promoting democracy* and *activating civil society/ broadening inclusion-media and education* found empirical support in the policies and thus could describe each national response towards disinformation in a convenient way. More specifically, Sweden's countermeasures, as described in policy documents, seem to be more in line with the suggested approaches than the German countermeasures. Germany's strategies, as described in the policy documents, are in this aspect more vague in relation to the aforementioned themes, which reiterates that the content is more limited and discreet. The shortcoming of these countermeasures in the German policies may show a weakness in itself compared to Wigell's suggestions of what strategies states could adopt to counter disinformation. Wijnja (2021) suggests that the German government hesitates to be sharing information and put focus on privacy issues, which can be related to cultural and historical aspects. Additionally, the reason why the issue of hybrid threats has not reached a broader societal audience is because the government focuses on increasing the resilience in the industry sector and the political sphere instead, as the German public is expected to act in a self-responsible manner (p.14).

The predominant findings are significant in that they clarify the similarities and differences in how Germany and Sweden communicate about countermeasures against disinformation in policy documents. Accordingly, the findings give an opportunity for clarifying and suggesting possible improvements.

It can be concluded that the Swedish policies have a higher level of informative content in contrast to the German ones. This poses an important question of the value and intention of policy documents to inform and raise awareness among societal actors and stakeholders like journalists, policymakers, politicians, researchers, and citizens. Consequently, as a contrast to Germany, the Swedish public can find more specific information and gain more profound knowledge of the problematic nature of disinformation and hybrid interference, which contributes to informs citizens on how to act against such threats. An additional aspect that clarifies the Swedish position better, is the comprehensive information on psychological defence, which is thoroughly elaborated on in the policies.

Consequently, this also raises the matter of how updated and consistent policy documents should be in order to communicate and describe the problems of disinformation and hybrid warfare and thereupon the related countermeasures. A report by the European Court of Auditors makes a pertinent case, namely that the EU action plan against disinformation 2018 "was relevant but incomplete" and that "the EU action plan has not been updated since 2018" (European Court of Auditors 2021. p.42). Although this is on the EU level, it demonstrates together with the findings from this paper that policy documents describing strategies against disinformation could be improved by being more consistent and updated for the sake of enhancing information for communicative and educational purposes in the work against disinformation and hybrid influences.

Considering the aforementioned, this research suggests that more comprehensive documents aimed for educational and awareness-raising purposes could be generated for the public in order to contribute with knowledge to fight against disinformation and hybrid

interference in the online environment and thus contribute with strengthening resilience in society.

Limitations

Considering the above-mentioned findings, what this paper has not determined, is the reason *why* the German policy documents are more vague in depicting national countermeasures. One explanation could be that Germany's strong relationship and historical ties with Russia, as well as the energy supply dependency, may have an impact on the diplomatic discourse and communication in policy documents regarding Russian foreign policy. In relevance to the aim of this research, the policy documents for Germany were more challenging to find. They were limited in their character, which shows that information about Germany's strategies for countermeasures might be communicated about on a more discreet level compared to Sweden's strategies. This has made it demanding to interpret and describe the German national strategy to the same extent as for Sweden. Further, we must bear in mind that policy documents may not show the entire picture of a country's strategy against disinformation and hybrid threats due to the secretive and classified nature of security strategies. Thus, it is difficult to establish what happens 'behind the curtains'.

Despite these limitations, the findings have served well to answer the research aim and the research question. In addition, the study gives a clear picture of describing both countries responses to disinformation influences emanating from Russia, and in addition hybrid interference in general. Although the findings show that the countermeasures are not explicitly applied towards Russia, it gives a comprehensive description of countermeasures against disinformation in general, which clearly is applicable to disinformation emanating from Russia.

Conclusion

This paper has clarified how Germany and Sweden respond to disinformation influences from Russia and thus contributed to a deeper understanding of how and in what way these countries describe and communicate countermeasures in primary policy documents on a specific and general level. The findings show that Germany and Sweden use partly similar countermeasures but also demonstrate differences in strategies to tackle disinformation. In the larger perspective, the research describes and nuances how hybrid interferences, especially disinformation, are managed on national levels and how governments communicate about them.

Future research is needed to establish *why* German policies are more discreet about countermeasures as described in policies, which could be clarified by conducting interviews with, for example, investigative journalists or experts in the field. In relation to that, another suggestion on this topic could look more closely into the federal states of Germany in order to emphasize how much federal politics influence strategies against hybrid interference. Moreover, it would be of value to research *why* Sweden, until now, has been holding back on possible regulations in relation to social media platforms, thus pointing out possible ways forward. At last, future studies could explore national regulatory measures against the complex and problematic information environment within the EU and thus clarify the balance between supranational regulatory actions and explore the importance and possibilities of national regulatory countermeasures.

References

Anckar, C. 2008. "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research". *Int. J. Social Research Methodology.* Vol. 11, No. 5, December 2008, p. 389–401. Accessed 16.10.2021 doi:10.1080/13645570701401552

Applebaum, A., Pomerantsev, P., Smith, M., Colliver, C. 2017. "Make Germany Great again" *Institute for Strategic Dialogue.* Accessed 13.10.2021 https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf

Barberá, P. 2019, "Social Media, Echo Chambers, and Political Polarization" in Persily, M. & Tucker, J.A. (2020). Social media and democracy. Cambridge University Press.

Bundesministerium der Verteidigung "Weißbuch, 2016- Zur sicherheitspolitik und zur Zukunft der Bundeswehr".. Accessed 03.11.2021 https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf

Bundesministerium des Innern 2016. "Verfassungsschutzbericht". Accessed 07.11.2021 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2016.pdf;jsessionid=A7F3470C981B000606BDD19CDACB8DED.1_cid373?__blob=publicationFile&v=4

Bundesministerium des Innern 2019. "Verfassungsschutzbericht". Accessed 07.11.2021 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2019-gesamt.pdf?__blob=publicationFile&v=10

Braun, V & Clarke, V. 2019. "Thematic analyses - a reflexive approach". The University of Auckland. Accessed 02.11.2021 at https://www.psych.auckland.ac.nz/en/about/thematic-analysis.html

Bowen, G. A. 2009. "Document Analysis as a Qualitative Research Method". *Qualitative Research Journal*, 9 (2), p. 27–40. Accessed 15.10.2021 https://doi.org/10.3316/QRJ0902027

Bundesministerium der Verteidigung, 2020. "Hybride Bedrohung: Fake News und Desinformation". Accessed 06.10.2021 https://www.bmvg.de/de/aktuelles/fake-news-und-desinformation-186254

Bundesregierung 2021. "Digitalisierung gestalten"Accessed 09.12.2021 https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002

Bundeszentrale für Politische Bildung 2021. "Dossier: Digitale Desinformation". Accessed 09.12.2021 https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/

Carlsson, U., 2018. "Medie- och informationskunnighet i den digitala tidsåldern- En Demokratifråga". Nordicom & Göteborgs universitet. Accessed 09.09.2021 https://www.nordicom.gu.se/sites/default/files/publikationer-hela-pdf/medie-_och_informationskunnighet_mik_i_den_digitala_tidsaldern_.pdf

Colliver, C., Pomerantsev, P., Applebaum, A., Birdwell, J. 2018. "Smearing Sweden International Influence Campaigns in the 2018 Swedish Election". *Institute for Strategic Dialogue*. Accessed 02.10.2021 https://www.isdglobal.org/isd-publications/smearing-sweden-international-influence-campaigns-in-the-2018-swedish-election/

Creswell, J.W. & Creswell, J.D. 2018. *Research Design: qualitative, quantitative and mixed methods approaches*. Thousand Oaks, California: SAGE publications.

Digital-made-in.de, 2021. "Strategische Kommunkiation im Wettbewerb der Narrative" accessed 10.12.2021 https://www.digital-made-in.de/dmide/vorhaben/wettbewerb-der-narrative-1794168)

Deverell, E. 2019. "Att identifiera och motstå informationspåverkan: En jämförande studie av hur de nordiska länderna organiserar arbetet", *Kungliga Krigsvetenskaps Akademiens Handlingar och Tidskrift*, (1), p. 31–54. Accessed 04.10.2021: https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=poh&AN=142098349&site=eds-live&scope=site

Durach, F., Bargaoanu, A., & Nastasiu, C. 2020. "Tackling disinformation: EU regulation of the digital space." *Romanian Journal of European Affairs*, 20(1), p. 5-20. Accessed 22.09.2021   https://eds-s-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=5&sid=7e6b51be-9eac-49fc-92f1-e1877ae7146d%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#db=edshol&AN=edshol.hein.journals.rojaeuf20.5

Doctrine of Information Security of the Russian Federation, 2016. Accessed 10.11.2021https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Durach, F., Bargaoanu, A. and Nastasiu, C., 2020. "Tackling Disinformation: EU Regulation of the Digital Space", *Romanian Journal of European Affairs*, 20 (1), pp. 5–20. Accessed 12.10.2021from   https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.rojaeuf20.5&site=eds-live&scope=site

Dunay, P., & Roloff, R., 2017. "Hybrid threats and strengthening resilience on Europe's eastern flank". George C. Marshall European Center for Security Studies. Accessed 11.10.2021 https://www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0

EUvsDisinfo, 2018. "Figure of the Week: 18.7 billion". Retrieved 08.10.2021 https://euvsdisinfo.eu/figure-of-the-week-18-7-billion/

EUvsDisinfo (2019). "Figure of the Week: 1.3 Billion". Retrieved 08.10.2021 https://euvsdisinfo.eu/figure-of-the-week-1-3-billion/

European Commision, 2018a. "Tackling online disinformation: a European Approach". Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 26.4.2018. Accessed 15.09.2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

European Commission 2018b. "Action Plan against Disinformation". Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Accessed 15.09.2021 https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

Euroepan Court of Auditors, 2021. "Disinformation affecting the EU: tackled but not tamed". Accessed 07.09.2021 https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=58682

European Parliament, 2019. "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States". Acessed 12.10.2021 https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

EU Commission (2016). "FAQ: Joint Framework on countering hybrid threats". Accessed 10.11.2021 https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250

EU Observer, n.d. "Germany 'main target' of Russian disinformation". Accessed 16.11.2021 https://euobserver.com/foreign/151177

Federal Ministry of Defence, 2020. Hybride Bedrohungen: Fake New und Desinformation. Accessed 17.11.2021 https://www.bmvg.de/de/aktuelles/fake-news-und-desinformation-186254

Galeotti, M. (2019) *Russian political war : moving beyond the hybrid*. First edition. Routledge/Taylor & Francis Group (Routledge Focus). Available at: https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=cat07147a&AN=lub.6367059&site=eds-live&scope=site

George, T. 2021. "A guide to exploratory research." Accessed 15.11.2021 https://www.scribbr.com/methodology/exploratory-research/)

Guess, A.M. & Lyons, B.A., 2020. "Misinformation, Disinformation, and Online Propaganda" in Persily, M. & Tucker, J.A. (2020). Social media and democracy. Cambridge University Press.

Hagelstam, A., 2018." Cooperating to counter hybrid threats". Accessed 19.11.2021 https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Hellman, M. & Wagnsson, C., 2017. "How can European states respond to Russian information warfare? An analytical framework". *European Security*, 2017 VOL. 26, NO. 2, p. 153–170. https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=13&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=000405867000001&db=edswss

Hellman, M., 2021. "Infodemin under pandemin- Rysk informationspåverkan mot Sverige". *Statsvetenskaplig Tidskrift*, 123(5), p. 451–474. Accessed 17.09.2021 https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=poh&AN=151988091&site=eds-live&scope=site

Hellman, M., 2021. "Infodemin under pandemin-Rysk informationspåverkan mot Sverige". *Statsvetenskaplig Tidskrift*; 2021, Vol.123 Issue 5, p. 451-474, 24p. Accessed 19.10.2021 https://eds-s-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=5&sid=cbb207b4-1bb9-4bf2-b69c-e6d1196e7b58%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=151988091&db=edo

Hoffman, F., 2007. "Conflict in the 21st century: The rise of hybrid wars". Potomac Institute for Policy Studies. Acccessed 19.10.2021
https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Humprecht, E., Esser, F. & Van Aelst, P., 2020. "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research', *International Journal of Press/Politics*, 25(3), p. 493–516. Accessed 15.09.2021 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=3&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edselc.2-52.0-85078187960&db=edselc

Hybrid CoE (n.d.) "What is Hybrid CoE". Accessed 10.11.2021 https://www.hybridcoe.fi/who-what-and-how/

Jankowicz, N., 2019. "Avoiding the Band Aid Effect in Institutional Responses to disinformation and hybrdi threats". The German Marshall Fund of the United States. Accessed 15.10.2021 https://www.gmfus.org/news/avoiding-band-aid-effect-institutional-responses-disinformation-and-hybrid-threats

Jaursch, J., 2019. "Regulatory reactions to disinformation". Stiftung Neue Verantwortung. Accessed 19.20.2021https://www.stiftung-nv.de/en/publication/regulatory-reactions-disinformation

Justitiedepartmementet 2016 (11:8). "Uppdrag till Statskontoret om svenska stattliga myndigheters verksamhet avseende psykologiskt förvsvar". Accessed 06.09.2021 https://www.regeringen.se/regeringsuppdrag/2016/09/uppdrag-till-statskontoret-om-svenska-statliga-myndigheters-verksamhet-avseende-psykologiskt-forsvar/

Justitiedepartementet 2018:80. ”En ny myndighet för Psykologiskt Försvar”. Accessed 10.09.2021 https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201880/

Kalniete, S. and Pildegovičs, T., 2021. ”Strengthening the EU's resilience to hybrid threats”, *European View*, 20 (1), pp. 23–33. Accessed 15.09.2021 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=11&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=150333962&db=poh

Knight, B. 2016. ” Teenage girl admits making up migrant rape claim that outraged Germany”. The Guardian. Accessed 02.01.2022 https://www.theguardian.com/world/2016/jan/31/teenage-girl-made-up-migrant-claim-that-caused-uproar-in-germany

Leung, L., 2015. ”Validity, reliability, and generalizability in qualitative research.” *Journal of Family Medicine and Primary Care*, 4(3), 324-327. Accessed 28.10.2021 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=5&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edsdoj.65a7e849988441390fd36d918d800cc&db=edsdoj

Library of Congress, 2021. ”Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech*”*. Retrieved from the, https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

Lowndes, V. Marsh, D., Stoker, G., 2018. *Theory and methods in political science*. Fourth edition (2018). Palgrave.

Mankoff, J. 2020. "Russian influence operations in Germany and theor effect". Center for Strategic Studies and International Studies. Accessed 13.10.2021 https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect

Martyr, K., 2021. ”Russian disinformation mainly targets Germany”*, EU report.* Deutsche Welle. Retrieved 13.09.2021 from https://www.dw.com/en/russian-disinformation-mainly-targets-germany-eu-report/a-56812164

Milmo, D., 2021. ”Frances Haugen takes on Facebook: the making of a modern US hero”. The Guardian. Accessed 12.10.2021 https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero

MSB, 2018. ”Countering information influence activites-a handbook for communicator.” Swedish Civil Contingencies Agency. Accessed 16.10.2021 https://www.msb.se/RibData/Filer/pdf/28698.pdf

MSB 2020. Medieberedskap. Accessed 30.11.2020 https://www.msb.se/contentassets/56c5b773737f47c7ad14809a52451c5b/faktablad-medieberedskap.pdf

MSB, 2021. "Psykologiskt Försvar". Accessed 21.11.2021
https://www.msb.se/psykologisktforsvar

Newman, N., Fletcher, R., Schulz, A., Andı, S., Robertson, C.T., Nielsen, R.K., 2021. Reuters Institute Digital News Report 2021. Accessed 06.11.2021 https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf

Pascu, I.M. & Vintila, N.-S., 2020. "Strengthening the Resilience of Political Institutions and Processes: A Framework of Analysis." *Connections QJ 19*, no. 3 p. 55-66 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=7&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=148601672&db=a9h

Regeringen, 2015a. "Uppdrag till Försvarsmakten och Myndigheten för samhällsskydd och beredskap avseende totalförsvarsplanering". Accessed 21.11.2021 https://www.regeringen.se/4ab3dd/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/regeingsbeslut-5-2015_12_10-uppdrag-till-forsvarsmakten-och-msb-avseende-totalforsvarsplanering.pdf

Regeringen 2015b. "Uppdrag till Försvarsmakten och Myndigheten för samhällsskydd och beredskap avseende totalförsvarsplanering". Accessed 21.11.2021 https://www.regeringen.se/regeringsuppdrag/2015/12/uppdrag-till-forsvarsmakten-och-myndigheten-for-samhallsskydd-ochberedskap-avseende-totalforsvarsplanering/

Regeringen, 2016. "Uppdrag till Statskontoret om svenska myndigheters verksamhet avseende psykologiskt försvar". Acccessed 15.10.2021 https://www.regeringen.se/regeringsuppdrag/2016/09/uppdrag-till-statskontoret-om-svenska-statliga-myndigheters-verksamhet-avseende-psykologiskt-forsvar/

Regeringskansliet, 2016. "Sveriges bidrag till en säkrare värld". Accessed 15.11.2021. https://www.regeringen.se/tal/2016/01/ums-tal-vid-folk-och-forsvar/

Regeringskansliet 2021. "Fortsatt satsning på ökad yttrandefrihet och motverkande av desinformation inom Östersjöregionen"Accessed 18.12.2021 https://www.regeringen.se/pressmeddelanden/2021/09/fortsatt-satsning-pa-okad-yttrandefrihet-och-motverkande-av-desinformation-inom-ostersjoregionen/

Renz, B. 2016. "Russia and 'hybrid warfare'. Contemporary Politics, Vol. 22, No. 3, 283–300. Accessed 17.09.2021 https://www.tandfonline.com/doi/full/10.1080/13569775.2016.1201316

Rhinard, M., 2017. "After the EU Global Strategy- Buiding resilience". *Institute for Security Studies*, pp. 25-27. Accessed 20.09.2021 https://www.iss.europa.eu/content/after-eu-global-strategy-%E2%80%93-building-resilience

Saurwein, F. & Spencer-Smith, C., 2020. "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe"*, Digital Journalism*, 8:6, 820-841, Accessed 16.09.2021 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=9&sid=db456a1b-f930-45e0-9aba-

ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%
3d#AN=edselc.2-52.0-85086279618&db=edselc

Seawright, J. & Gerring, J., 2008. "Case Selection Techniques in Case Study Research, Political Research Quarterly", 61(2), 294-308. Accessed 27.10.2021 https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/pdfviewer/pdfviewer?vid=8&sid=cbbaff18-25d8-49e0-abbc-92c14a9260e0%40redis

Spiegel, 2016. "Russia's Propaganda Campaign Against Germany". Accessed 02.01.2022 https://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html

Speck, D., 2020. "EBU Media Intelligence Service". Trust in Media 2020. Accessed 06.11.2021 https://medienorge.uib.no/files/Eksterne_pub/EBU-MIS-Trust_in_Media_2020.pdf

Statskontoret 2017:5. "Myndigheternas arbete med psykologiskt försvar". Accessed 10.09.2021 https://docplayer.se/48281826-2017-5-myndigheternas-arbete-med-psykologiskt-forsvar.html

Statens Medieråd, 2020. "Lägesrapport 2020". Accessed 16.11.2021 https://www.statensmedierad.se/download/18.5fbaa484175c8720dd740eeb/16068398248 75/Statens%20medier%C3%A5ds%20l%C3%A4gesrapport%202020%20med%20bilaga. pdf

Stegers, F., 2020. "Desinformation in Deutschland. Gefahren und mögliche Gegenmaßnahmen aus Sicht von Fachleuten". University of Applied Sciences Hamburg on behalf of the Vodafone Foundation Germany. Accessed 14.09.2021 https://www.vodafone-stiftung.de/wp-content/uploads/2021/07/Studie_Vodafone-Stiftung_Desinformation-Expertenbefragung.pdf

Statsrådsberedningen, 2018. "Stärkt psykologiskt försvar och åtgärder mot påverkansoperationer". Regeringskansliet. Accessed 15.11.2021 https://www.regeringen.se/artiklar/2018/01/starkt-psykologiskt-forsvar-och-atgarder-mot-paverkansoperationer/

Sturm, D.F., 2016. "So hilft Deutschland im Kampf gegen Kreml-Propaganda". Accessed 12.11.2021 https://www.welt.de/politik/deutschland/article155749415/So-hilft-Deutschland-im-Kampf-gegen- Kreml-Propaganda.html

Sundberg, S., 2021. "Behöver vi oroa oss för desinfomration?". Internetkunskap. Accessed 13.09.2021 https://internetkunskap.se/desinformation/behover-vi-oroa-oss-for-desinformation/

Sängerlaub, A. 2018. "Feuerwehr ohne Wasser? Möglichkeiten und Grenzen des Fact-Checkings als Mittel gegen Desinformation". Stiftung Neue Verantwortung. Accessed 11.10.2021 https://www.stiftung-nv.de/de/publikation/feuerwehr-ohne-wasser-moeglichkeiten-und-grenzen-des-fact-checkings-als-mittel-gegen

Vaccari, C., n.d. "Online Mobilization in Comparative Perspective: Digital Appeals and Political Engagement in Germany, Italy, and the United Kingdom", *Political Communication*, 34(1), p. 69–88. https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=17&sid=db456a1b-f930-45e0-9aba-

ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d% 3d#AN=edselc.2-52.0-84992418608&db=edselc

Wagnsson, C. Barzanje, C., 2021. "A framework for analysing antagonistic narrative strategies: A Russian tale of Swedish decline". *Media, War & Conflict*, Vol. 14(2) p. 239–257. Accessed 11.10.2021 https://journals.sagepub.com/doi/10.1177/1750635219884343

Wijnja, K., 2021. "Countering hybrid threats: does strategic culture matter?", *Defence Studies,* Accessed 06.11.2021 https://www.tandfonline.com/doi/full/10.1080/14702436.2021.1945452

Wigell, M., 2021. "Democratic Deterrence: How to Dissuade Hybrid Interference", *The Washington Quarterly*, 44:1, p. 49-67, https://eds-p-ebscohost-com.ludwig.lub.lu.se/eds/detail/detail?vid=19&sid=db456a1b-f930-45e0-9aba-ea700ce59ca7%40redis&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d% 3d#AN=149454682&db=edb

Yin, R. K., 1994. "Case study research: Design and methods" (2nd ed.). Thousand Oaks, CA: Sage.

Appendix

The documents for the keyword analyses are available upon request as they could not be included here by reason of their format.